Band 9 / 2021

Das Social Engineering Dilemma

Warum Unternehmen trotz Schulungsmaßnahmen Opfer von Social Engineering Angriffen werden

Michael Suker

Schriftenreihe der
Landesverteidigungsakademie

Schriftenreihe der
Landesverteidigungsakademie

Michael Suker

Das Social Engineering Dilemma

Warum Unternehmen trotz Schulungsmaßnahmen Opfer von Social Engineering Angriffen werden

9/2021
Wien, September 2021

Impressum:

Medieninhaber, Herausgeber, Hersteller:
Republik Österreich / Bundesministerium für Landesverteidigung
Rossauer Lände 1
1090 Wien

Redaktion:
Landesverteidigungsakademie
Zentraldokumentation
Stiftgasse 2a
1070 Wien

Schriftenreihe der Landesverteidigungsakademie

September 2021
ISBN 978-3-903359-33-8

Druck:
ReproZ W 21-xxxx
Stiftgasse 2a
1070 Wien

Inhaltsverzeichnis

Das Social Engineering Dilemma:

Warum Unternehmen trotz Schulungsmaßnahmen Opfer von Social Engineering Angriffen werden.

Kurzfassung

Informations- und Kommunikationstechnologie (IKT) hat das Leben der Menschen verändert. Stark ansteigende Digitalisierung und die Vermischung von Arbeitsumgebung und Privatleben durch dezentrale IT-Infrastruktur brachten für Arbeitgebende sowie Arbeitnehmende zusätzliche neue Möglichkeiten einer modernen Arbeitskultur und Umgebung.

Der ständige Zuwachs neuer IKT-Systeme und Technologien brachte aber auch viele neue Gefahren durch verschiedenste Angriffsvektoren. Technische Abwehrmaßnahmen werden kontinuierlich neu entwickelt, um Einfallstore für Angriffe bestmöglich zu schließen. Leider wird der Mensch als wesentlicher Faktor der Informationssicherheit wenig beachtet. Diese Angriffsart, die durch geschickte Täuschung und Manipulation des Menschen vorhandene technische Schutzmaßnahmen umgeht, nennt sich Social Engineering.

Diese Studie beschäftigt sich mit der explorativen Fragestellung warum Unternehmen trotz umgesetzter Schulungsmaßnahmen Opfer von Social Engineering Angriffe werden. Um diese Forschungsfrage zu beantworten, wurde der qualitative Forschungsprozess ausgewählt. Für die Datenauswertung wurde eine strukturierte Inhaltsanalyse der relevanten Literatur durchgeführt, um eine Grundlage für den aktuellen Stand des Wissens in Bezug auf Social Engineering zu schaffen.

Durch Interviews von acht ausgewählten Sicherheitsexperten, welche anhand der qualitativ strukturierten Inhaltsanalyse ausgewertet wurden, konnte ein repräsentativer Querschnitt erforscht werden, um abschließend Handlungsempfehlungen zur Implementierung und Risikominimierung von Social Engineering Gefahren in Unternehmen ableiten zu können.

Die Ergebnisse zeigen, dass es dringenden Handlungsbedarf für organisatorische Maßnahmen in den Unternehmen gibt. Den Sicherheitsverantwortlichen muss mehr Autonomie bei der Prozessmodellierung eingeräumt werden.

Insbesondere das fehlende Verständnis der Mitarbeiterinnen und Mitarbeiter für die Gefahren von Social Engineering sollte als größtes Risiko adressiert werden, welches nur durch praxisnahe, speziell auf das Unternehmen abgestimmte Sicherheitsschulungen und die zusätzliche Implementierung einer Sicherheitskultur gemessen an Reifegraden abgeschwächt werden kann. Abschließend wurden organisatorische Handlungsempfehlungen abgeleitet.

Diese Studie zeigt auf, dass Verantwortliche in Unternehmen einen stärkeren Fokus auf die Sensibilisierung der Mitarbeiter legen müssen. Der Einsatz von kontinuierlich aktualisierten Personalschulungen mit einem stärkeren Praxisbezug zu Social-Engineering-Angriffen sollte in zukünftigen Untersuchungen evaluiert werden. Dies kann jedoch nur durch ein ausreichendes Verständnis der Mitarbeitenden für die Bedrohungen und mit der Unterstützung durch die Geschäftsleitung erreicht werden.

Abstract

Information and communication technology has changed everyone's lives. Rapidly increasing digitization through decentralized information and communication technology (ICT) provides additional opportunities for a modern work culture and environment. However, the constant development of new ICT systems and technologies offers attackers many new attack vectors, which are prevented with the help of increasingly sophisticated technical measures. Unfortunately, not enough attention is paid to the individual human being, who is an essential factor in information security. The type of attack in which people are exploited through sophisticated manipulation is known as social engineering. In order to address this exploratory research question, the qualitative research process was selected. To answer the research question, a structured content analysis of the relevant literature was conducted to prepare an overview of the current state of knowledge related to social engineering. By conducting expert interviews with eight selected information security experts working in the ICT sector, which were evaluated by qualitative structured content analysis, a representative sample could be researched to derive recommendations for further action.

The results show that there is an urgent need for improvement among company management in all sizes and sectors. Security managers must be granted increased autonomy in process modeling. In particular, the lack of understanding of the dangers can be addressed as the greatest risk, which could only be mitigated by practical security training specifically adapted to the company and the additional implementation of a security culture with maturity levels. Recommendations for improvement resulting from the research are finally derived. In summary, it is recommended to focus more on making the employees more aware of the dangers of social engineering. The use of continuously updated employee training with a more practical focus on social engineering attacks should be evaluated in future research. However, this can only be achieved by sufficient understanding of the threats and support from the management.

1 Einleitung

Die Informationstechnologie und Kommunikationstechnologie (IKT) hat sich zu einem festen Bestandteil unserer Gesellschaft entwickelt. Es existiert fast keine Branche, in der die Informationstechnologie (IT) nicht genutzt wird. Jedoch kann diese Technologie, die wir nutzen, auch dazu verwendet werden, um der Gesellschaft Schaden zuzufügen. Informationssicherheit ist eine der am stärksten wachsenden Herausforderungen, der sich Unternehmen gegenwärtig stellen müssen und die sie zu bewältigen haben (Aldawood, 2019; Thai & Sajal, 2020).

Stark ansteigende Digitalisierung und die Vermischung von Arbeitswelt und Privatleben durch zunehmende Dezentralisierung der Informations- und Kommunikations- Infrastruktur infolge von Homeoffice sind einer der Gründe, warum Angriffe auf die Informationssicherheit zunehmen.

Der ständige Bedarf und Zuwachs an Informationssystemen bringt auch immer neue Technologien zur technischen Bekämpfung von Gefahren und zur Schließung von neu auftretenden Sicherheitslücken. Angreifende haben es zunehmend schwerer, die implementierten technischen Schutzmaßnahmen zu überwinden und benötigen manchmal andere Methoden und Wege, um diese Schutzmaßnahmen zu umgehen (Thai & Sajal, 2020).

Eine der größten Bedrohungen geht von einer Angriffsart aus, bei der stets der Mensch durch geschickte Manipulation getäuscht wird, um an die gewünschten Ziele zu gelangen. Diese Angriffsart zur Informationsgewinnung, welche auf die Schwachstelle Mensch abzielt, nennt man Social Engineering (Drechsler, 2019). Dabei nutzt die Angreiferin bzw. der Angreifer Social Engineering als Angriffsvektor, um mithilfe von menschlichen Wesensmerkmalen, wie etwa Hilfsbereitschaft oder Vertrauen, an Zugangsdaten zu gelangen oder unbemerkt Schadsoftware in das Firmennetzwerk einzuschleusen. Sehr oft stehen dahinter finanzielle Interessen (Franz & Benlian, 2020).

Der Social Engineer praktiziert durch die spezielle Kunst der Täuschung eine der effektivsten Methoden zur Kompromittierung von Computersystemen, wovon sowohl Privatpersonen, Unternehmen in allen Betriebsgrößen als auch staatliche Organisationen betroffen sein können (BSI - G 0 Elementare Gefährdungen - IT-Grundschutz-Kataloge - G 0.42 Social Engineering, 2011).

Er untersucht die Geschäftsprozesse sowie Kommunikationsstrukturen und versucht, sowohl mit diversen analogen als auch mit technischen Hilfsmitteln und Methoden zur Ausnützung menschlicher Schwäche an seine vorher definierten Ziele zu gelangen. Der Mensch wird dabei als das schwächste Glied in der Informationssicherheitskette ausgenützt (Franz & Benlian, 2020; Klipper, 2020).

> *„There is no technology today that cannot be defeated by social engineering - Frank Abagnale"* (Wright, 2016).

Ein aktueller Sicherheitsvorfall im Rahmen einer nicht öffentlichen Videokonferenz der EU-Verteidigungsminister zeigt, dass auch hochrangige Politikgrößen und deren Social Media Teams trotz intensiver Awareness Schulung Opfer von Social Engineering werden können.

Vor der Videokonferenz wurde ein Foto von der niederländischen Verteidigungsministerin über den Social-Media-Kanal Twitter mit den geheimen Zugangscodes der Konferenz veröffentlicht. Ein niederländischer Journalist hat diese Sicherheitslücke aufgezeigt und aktiv für mehrere Minuten an der Konferenz teilgenommen (Frankfurter Allgemeine, 2020).

Während der Covid-19 Pandemie konnten viele Social Engineering Kampagnen wahrgenommen werden, bei denen staatliche Soforthilfemaßnahmen nachgebildet wurden. Nachdem die betroffenen Unternehmen die für die Hilfsmaßnahmen spezifischen Daten auf der täuschend echt aussehenden Seite hochgeladen hatten, konnten die Angreifer sich selber als Antragstellende kennzeichnen und zu ihren Gunsten die staatliche Soforthilfe beantragen (BSI für Bürger - Informationen - Vorsicht Phishing: Die Corona-Krise als Köder, 2020).

Im Jahresbericht der Agentur der Europäischen Union für Cybersicherheit (ENISA) wurde festgestellt, dass durch eine Angriffsart des Social Engineering, die Business Email Compromise[1] oder auch CEO Fraud, zwischen 2016 und 2019 weltweit über 26 Milliarden US Dollar an Schaden angerichtet wurde (ENISA ETL Report 2020 - Phishing (EN), 2020). Der österreichische Luftfahrtzulieferer FACC verlor 2016 durch einen CEO Fraud mindestens 50 Millionen Euro (FACC-Betrug, 2016).

1.1 Problemstellung

Security Awareness ist als dynamischer Prozess zu verstehen, bei dem die Belegschaft und die Sicherheitsbeauftragten von Unternehmen immer wieder vor neuen Herausforderungen stehen (Franz & Benlian, 2020). Die steigende Komplexität und zunehmende Automatisierung der Angriffe machen es schwieriger, Mitarbeiterinnen und Mitarbeiter auf alle Social Engineering Attacken vorzubereiten. Durch Bewusstseinssteigerung und Verständnisentwicklung über die Arbeitsmuster, Phasen und Tools aus der Perspektive der Angreiferin bzw. des Angreifers kann dieses Risiko dennoch minimiert werden (Franz & Benlian, 2020; IONOS, 2020).

Viele Unternehmen und Organisationen entwickelten daher eigene Awarenessprogramme, um sich selbst und ihre Mitarbeitenden vor Social Engineering zu schützen.

Selbst kurz nach den Awareness-Trainings öffneten einige Mitarbeiter PDF-Dateien mit Schadsoftware. Oft ist dieses Fehlverhalten den gelebten und validen Geschäftsprozessen geschuldet.

Auch Sicherheitsparadigmen wie Security bzw. Privacy By Design[2] sind im realen Betrieb wirkungslos, wenn nur technische Fehler berücksichtigt werden, aber menschliches Fehlverhalten Sicherheitsvorfälle auslösen (Klipper, 2020).

[1] Der Angreifer verschafft sich Zugang zu einem E-Mail-Konto des Unternehmens, um Kunden oder Mitarbeiter zu täuschen

[2] Systeme schon bei ihrer Entwicklung möglichst unempfindlich gegen Angriffe und Fehler zu entwerfen

Da durch Social Engineering Angriffe jährlich Schäden in Milliardenhöhe angerichtet werden, kann man davon ableiten, dass Sicherheitsschulungen alleine nicht ausreichen und ergänzende Ansätze in Bezug auf Social Engineering Schutzmaßnahmen entwickelt werden müssen.

Das FBI veröffentlichte im April 2020 eine Warnung, dass Cyber-Akteure infolge der Covid-19 Pandemie verstärkt Schwachstellen in Systemen und Prozessen ausnützen, um Unternehmen und Personen Schaden zuzufügen. Die verschiedensten Angriffsvektoren, wie etwa gefälschte Webseiten oder Phishing Kampagnen richteten sich besonders auf vertrauliche Informationen und Finanztransaktionen, die aufgrund der Lockdown Maßnahmen von den Mitarbeitenden mittels Remote-Verbindungen zu den Unternehmensnetzwerken sowie diversen Kommunikationsdiensten genutzt und von den Angreifenden kompromittiert wurden (*Cyber Actors Take Advantage of COVID-19 Pandemic to Exploit Increased Use of Virtual Environments*, 2020).

Die Rolle des CISO[3] in der Organisation wird aufgrund der durch die Pandemie erzwungenen Änderungen der Geschäftsprozesse sowie Unternehmensstandards, wie beispielsweise Remotezugriff für alle Mitarbeiterinnen und Mitarbeiter, Cloud-Technologien und andere Methoden für den mobilen Datenaustausch immer wichtiger und entwickelt sich stetig weiter.

Sicherheitsverantwortliche sollten bei der Implementierung einer der flexiblen Bedrohungslage angepassten Sicherheitskultur nicht nur strategisch direkt der Unternehmensleitung unterstellt werden, sondern auch bei der Identifizierung und Neubewertung der Geschäftsstrategien und ihren Auswirkungen proaktiv eingebunden werden (PwC, 2020).

Um Gefahren zu minimieren und etwaige Opfer in Unternehmen bestmöglich zu schützen, ist eine Einflussnahme von CISO´s und Sicherheitsbeauftragten auf alle Prozesse in der Organisation notwendig. Diese Vorgehensweise wird jedoch von den meisten Organisationen erbittert boykottiert. Informationssicherheit wird immer noch als Hindernis empfunden (Klipper, 2020; PwC, 2020).

[3] Ein Chief Information Security Officer (CISO) bezeichnet die Rolle des für Informationssicherheit Gesamtverantwortlichen in einer Organisation.

1.2 Zielsetzung und wissenschaftliche Fragestellung

Folgende Forschungsfrage wird im Rahmen dieser Publikation untersucht:

Aus welchen Gründen werden Unternehmen trotz umgesetzter Schulungsmaßnahmen Opfer von Social Engineering Attacken?

Ziel der Publikation:

Zielsetzung dieser wissenschaftlichen Arbeit ist es, durch explorative, semi-strukturierte Experteninterviews von Sicherheitsverantwortlichen in staatlichen Organisationen sowie Betreiberinnen und Betreiber kritischer Infrastruktur einen repräsentativen Querschnitt betreffend die Ursachen von Social Engineering zu erforschen. Auf Basis der Ergebnisse wird eine Handlungsempfehlung zur Implementierung von organisatorischen Schutzmaßnahmen abgeleitet.

2 Grundlagen

Social Engineering ist keineswegs neu. Einer der berühmtesten Social Engineering Angriffe fand schon in der Antike statt. Das antike Heldenepos "Die Odyssee" des griechischen Dichters Homer beschreibt ein hölzernes Pferd, welches von den Griechinnen und Griechen gebaut und als Zeichen der Unterwürfigkeit den siegreichen Trojanerinnen und Trojanern übergeben wurde. In den Nachtstunden überfielen etwa 30 griechische Elitesoldaten, die sich im Bauch des hölzernen Pferdes versteckt hatten, die Stadt. Seither wird der Begriff „Trojanisches Pferd“ sinnverwandt mit "etwas vortäuschen" gleichgesetzt und auch als Bezeichnung für eine spezielle Form von Schadsoftware verwendet (Gray, 2018).

Ein anderes bekanntes Beispiel eines Social Engineering Angriffes ist die Geschichte des Hauptmannes von Köpenick, der mit einer gestohlenen Soldatenuniform und schneidigem militärischen Auftreten seine Opfer durch den Einsatz von Autorität manipulierte und sich so Zugang zur streng bewachten Stadtkasse verschaffen konnte (Pokupec & Schmitz, 2020; S. Schumacher, 2014).

Einer der gefürchtetsten Cyberkriminellen der 80er und 90er-Jahre in den Vereinigten Staaten von Amerika (USA) war Kevin Mitnick. Nachdem er im Jahr 1995 wegen unzähliger Attacken auf Computersysteme verurteilt und nach einer Haftstrafe im Jahr 2000 entlassen wurde, wechselte er die Seite und arbeitet gegenwärtig als Sicherheitsberater für das FBI und viele weitere Unternehmen. In seinen zahlreichen Fachbüchern über Social Engineering beschreibt er "Die Kunst der Täuschung". Seine Werke sind Leitliteratur für viele weitere Forschungen zu dieser Thematik (Khin, 2016; Schwan, 2008).

Die Angriffsmethode Social Engineering nutzt viele psychologische Verhaltensmuster der Menschen sowie deren Kommunikationswege.

Die steigende Komplexität der Geschäftsprozesse ermöglicht es den Angreiferinnen und Angreifern, durch geschickte Täuschung und Legendierung[4] Ausnahmesituationen in den Geschäftsprozessen auszunützen, die schließlich von den betroffenen Mitarbeiterinnen und Mitarbeitern legitimiert werden.

Besonders entscheidend ist die Authentizität der Sender und Empfänger bei den Schnittstellen in Prozessen. Deren Schwachstellen der Senderauthentizität nutzen Social Engineers mit diversen Kommunikationsmitteln aus, die nicht in den Prozessen vorgesehen sind (Fox, 2014). Auch die unterschiedlichen Angreifenden und deren Motivationen sind sehr vielfältig. In diesem Kapitel werden die notwendigen Grundlagen und was diese besondere Angriffsmethode so erfolgreich macht, detailliert betrachtet.

> *„Wenn du deinen Feind kennst und dich selbst kennst, brauchst du das Ergebnis von 100 Schlachten nicht zu fürchten"* (Sun Tzu, o. J.)

2.1 Social Engineering im modernen Zeitalter

Gemäß Cambridge Dictionary wird der Begriff Social Engineering in zwei unterschiedliche Begriffsbestimmungen unterteilt.

In der ersten Begrifflichkeit stammt Social Engineering aus der Politikwissenschaft und wird als eine künstliche Steuerung oder Veränderung einer Gesellschaft bezeichnet (SOCIAL ENGINEERING | Bedeutung im Cambridge Englisch Wörterbuch, 2020). Etzemüller (2017) beschreibt Social Engineering als einen neuen Begriff für Menschenführung und Entscheidungsarchitekturen, um Menschen so zu beeinflussen, dass sie selbst ihre Lebenseinstellung verbessern können (Etzemüller & Zentrum Für Zeithistorische Forschung Potsdam, 2017).

Der zweite Terminus verortet Social Engineering im Kontext der Informationssicherheit. Hier hat der Begriff jene Bedeutung, die eine Taktik beschreibt, durch die Menschen verleitet werden, geheime oder persönliche Informationen zu offenbaren und damit Schaden herbeiführen.

[4] Vortäuschen eines Sachverhaltes. Häufig die Biografie einer Person oder Objekt.

Selbst Computersysteme, die durch Firewalls geschützt sind, können dem Social Engineering zum Opfer fallen (SOCIAL ENGINEERING | Bedeutung im Cambridge Englisch Wörterbuch, 2020).

Nachdem in den 1960er-Jahren die öffentliche Nutzung von Computer Netzwerken aus dem Arpanet, einem wissenschaftlichen Netzwerk von Bildungsinstituten entwickelt wurde, entstand auch das Paradigma der Informationssicherheit im Kontext der Cybersicherheit.

Technikaffine Personen nutzten in den 1970er-Jahren ihr Wissen und ihre Überzeugungsfähigkeit, um Telefonnetzwerke zu manipulieren und sich unautorisiert Zugang zu Leitungen zu verschaffen, die ursprünglich nur technischen Fachkräften der Telefongesellschaften vorbehalten waren. Die sogenannten Phone Phreaker konnten so kostenlos telefonieren.

Die benötigten Zugangsinformationen erhielten sie dabei von ahnungslosen Angestellten der Telefongesellschaften, indem sie sich selbst als Telefontechniker legitimierten. Der Begriff Social Engineering entstand aus der Phone Phreaking Community und wurde als Bezeichnung für die Täuschung der Angestellten verwendet (Hatfield, 2018).

2.2 Informationssicherheit

Ein wesentlicher Bestandteil der Wertschöpfungskette von Unternehmen und Organisationen sind Informationen. Datendiebstahl kann für ein Unternehmen existenzbedrohend sein (BSI - IT-Grundschutz-Kompendium - 1 IT-Grundschutz – Basis für Informationssicherheit, 2020, Kapitel 1.1).

IT-Unterstützung ist ein wesentlicher Bestandteil bei der Bearbeitung von Geschäftsprozessen. Diese sorgen für neue Möglichkeiten zur Senkung von Transaktionskosten und Beschleunigung von Abläufen, bieten jedoch für Angreifer viele Angriffsvektoren, da die IT-Systeme der Unternehmen und Organisationen oft nur unzureichend geschützt werden (Fox, 2014).

Im europäischen Raum existieren unterschiedliche Standardwerke für die Implementierung eines umfassenden Informationssicherheitsmanagementsystems (ISMS).

Die Normenreihe ISO/IEC 27001 und der Grundschutz des deutschen Bundesamtes für Sicherheit in der Informationstechnik (BSI) gehören zu den weitverbreitetsten Werken (Österreichisches Informationssicherheitshandbuch, 2020a).

Die verschiedenen Schutzziele im Bereich der Informationssicherheit werden im BSI Grundschutz und in der ISO/IEC 27001 Norm in folgende drei Kategorien bzw. Säulen zugeordnet (BSI - IT-Grundschutz-Kompendium - 1 IT-Grundschutz – Basis für Informationssicherheit, 2020).

Verfügbarkeit: Geschäftsprozesse, die abhängig von IT-Systemen sind, können beeinträchtigt bzw. nicht weitergeführt werden, wenn das benötigte IT-System nicht erreichbar ist oder die erforderlichen Datenbestände nicht verfügbar gemacht werden können. Systemausfälle können für Unternehmen existenzbedrohende Auswirkungen auslösen.

Vertraulichkeit: Die für Unternehmen essenziellen Informationen dürfen nur von Personen verfügbar gemacht werden, die tatsächlich dazu berechtigt sind. Auch bei der Übertragung von Daten muss sichergestellt werden, dass die Informationen entsprechend verschlüsselt versendet werden und nur durch berechtigte Personen entgegengenommen bzw. geöffnet werden können.

Integrität: Informationen dürfen nicht unerkannt verändert oder verfälscht werden. Dies könnte in Unternehmen zu schwerwiegenden Fehlern in Geschäftsprozessen führen, wie etwa falsche Zahlungsanweisungen, falsche Lieferungen oder fehlerhafte Produkte.

Die nachfolgende Abbildung 2.1 stellt mögliche Auswirkungen von Social Engineering Angriffen auf Unternehmen dar. Aldawood (2019) unterteilt die Auswirkungen auf Unternehmen in störende und ausbeuterische Aktivitäten.

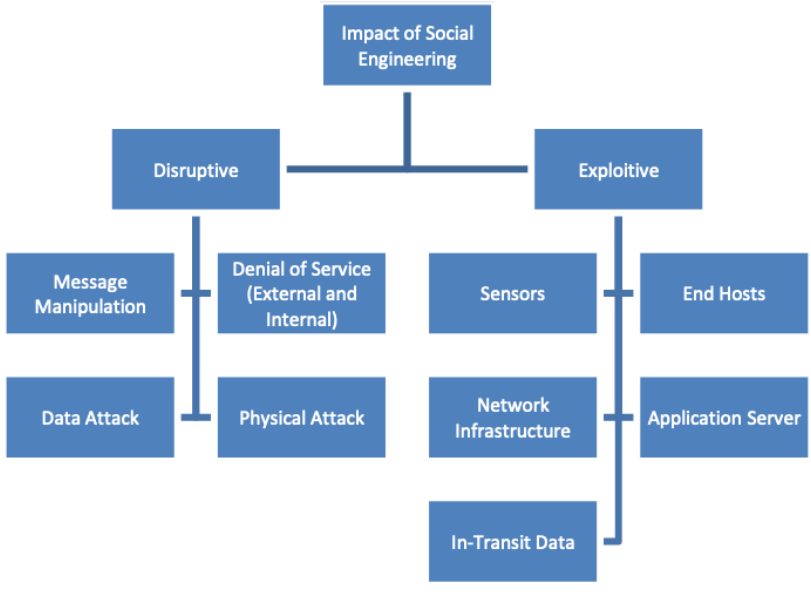

Abbildung 2.1: Auswirkungen von Social Engineering auf Unternehmen (Aldawood, 2019)

Bei Angriffen auf Unternehmen versucht der Social Engineer durch die Mitarbeiter an Informationen zu kommen. Die Auswirkungen können zum Reputationsverlust der Organisation oder zu einem vollständigen Produktionsausfall führen (Aldawood, 2019).

2.3 Arten von Angreiferinnen und Angreifern

Es gibt viele verschiedene Arten von Angreiferinnen und Angreifern. Nicht alle haben finanzielle Interessen oder böswillige Absichten. Welche verschiedenen Typen von Social Engineers existieren und welche Ziele sie haben, wird in diesem Unterkapitel beleuchtet.

Hacker: Hacker sind grundsätzlich technisch ausgesprochen versiert und haben die Absicht, in fremde Computersysteme oder Netzwerke einzudringen. Da Soft- und Hardwarehersteller versuchen, ihre Produkte so sicher wie möglich zu programmieren bzw. zu erzeugen, suchen Hacker oft nach anderen Methoden und Taktiken, um in fremde Systeme einzudringen (Luber & Schmitz, 2017b). Eine sehr effektive Methode dafür ist Social Engineering.

Erstmals wurde der Begriff „Hacker“ in den 50er-Jahren im sogenannten Jargon File definiert und als eine Person beschrieben, die eine intellektuelle Herausforderung sucht und deshalb fremde Computersysteme angreift. Böswillige Hacker, die sich nicht an den Ehrenkodex der Hacker halten, werden als „Cracker“ oder manchmal auch Black Hat Hacker oder Cyberpunk bezeichnet (M. Schumacher, 2013; Stirnimann, 2018).

Penetrationstester: Sie besitzen die gleichen technischen Fähigkeiten wie Hacker, haben aber keine bösen Absichten. Penetrationstester auch Pen-Tester oder White Hat Hacker genannt, nutzen ihr Können, um Sicherheitslücken aufzuzeigen (Hadnagy, 2011, S. 39). Durch Penetrationstests versuchen die Spezialistinnen und Spezialisten mit allen zu Verfügung stehenden Angriffsmethoden, aber mit Bewilligung der zu testenden Organisation, in deren Systeme einzudringen. Dabei kommen auch Social Engineering Taktiken und Tools zum Einsatz. Die genau protokollierten Informationen über erkannte Schwachstellen in Soft- und Hardware teilen sie mit ihren Auftraggeberinnen und Auftraggebern, aber auch mit Fachzeitschriften (Luber & Schmitz, 2017a).

Spione: Spionage ist das heimliche Sammeln von Informationen, um sich einen strategischen oder finanziellen Vorteil zu verschaffen. Der Angriffsschwerpunkt liegt oft auf Wirtschaftsspionage von Unternehmen. Eine der wichtigsten Disziplinen des Spiones ist das Social Engineering. Spione trainieren dieses Handwerk perfekt, um ihre Opfer täuschen zu können (Hadnagy, 2011, S. 39; „Spies and Espionage“, 2020).

Innentäter: Mitarbeiter einer Organisation, besonders jene, die über ausreichend Wissen über betriebsinterne Verfahren, Prozesse oder Schwachstellen verfügen, gelten als große Gefahr für Unternehmen.

Laut einer Studie werden weltweit über 60 % aller Cyberangriffe von Innentätern ausgeführt. Oft werden frustrierte Mitarbeiterinnen und Mitarbeiter kriminell. Insider können aber auch Kundinnen und Kunden, Vertragsparteien, Lieferantinnen und Lieferanten oder beratende Personen sein.

Weber et al. (2020) unterscheiden Innentäter in zwei Gruppierungen. Insider, die ohne Absicht bzw. ohne Kenntnis dem Unternehmen Schaden zufügen und jene, die bewusst Informationen abfließen lassen (Brandt, 2016; Weber et al., 2020).

Es existieren viele unterschiedliche Motive und Auslöser für Sicherheitsvorfälle durch Social Engineering von Innentätern in Unternehmen. Nachrichtendienste oder Wirtschaftsspione nutzen diese Zielgruppe zur Informationsgewinnung. Bei der Anwerbung von Innentätern für kriminelle Zwecke wird nach dem MICE-Prinzip vorgegangen. Das englische Akronym MICE steht für die wichtigsten Lockmittel und Beweggründe von Innentätern (Fleischer, 2016).

Money (Geld): Ein zusätzliches Einkommen ist notwendig, um den exzessiven Lebensstil weiterzuführen.

Ideology (Ideologie): Kriminelle aus ideologischer Überzeugung.

Coercion (Zwang): Häufig werden Mitarbeiter mit einer Enthüllung von privaten Informationen erpresst.

Ego: Frustration ist einer der Faktoren, um sich von anderen Mitarbeiterinnen und Mitarbeitern abzuheben.

Im Falle des im Jahr 2020 verurteilten österreichischen Bundesheer Oberst im Ruhestand, der über 20 Jahre für russische Geheimdienste operiert hat, sollen bis zu 280 000.- Euro von seinem russischen Verbindungsoffizier gezahlt worden sein (Bischof, 2020).

Identitätsdiebe: Beim Identitätsdiebstahl werden persönliche Informationen wie Name, Bankdaten, Adressen und sonstige Daten ohne Wissen der Eigentümerin bzw. des Eigentümers für kriminelle Zwecke verwendet. Die Täter verwenden dabei viele Methoden des Social Engineerings. In der bereits in der Einleitung dieses Kapitels erwähnten Geschichte von Hauptmann Köpenick wurde ein Identitätsdiebstahl umgesetzt, indem die gestohlene Uniform zur Verkörperung einer anderen Identität verwendet wurde (Hadnagy, 2011, S. 39).

In den 1960er-Jahren gelang es Frank Abagnale, interne Betriebsinformationen über die Branchenterminologie von Fluglinien, insbesondere die der U.S Fluglinie PanAm zu sammeln, indem er sich als Redakteur einer Schülerzeitung ausgab. Nachdem er mit einer gestohlenen Pilotenuniform kostenlos fliegen konnte und sich im Laufe der Zeit mehr Informationen über das Gehaltsauszahlungssystem von PanAm aneignen konnte, hatte er genug Fachwissen, um interne Gehaltsschecks zu fälschen und diese einzulösen. Die Geschichte von Frank Abagnale wurde im Hollywood Streifen "Catch Me If You Can" verfilmt (Nathaniel, 2018).

Regierungen: Social Engineering kann auch von Regierungen eingesetzt werden, um ihre Bürger zu kontrollieren, zu manipulieren oder um Informationen verbreiten zu können. Durch Social Engineering Methoden können diese Informationen unter Umständen besser von der Bevölkerung als glaubwürdiger wahrgenommen werden (Hadnagy, 2011, S. 40).

2.4 Motivation und Ziele der Angreiferinnen und Angreifer

Das Verständnis der unterschiedlichen Motivationen der Angreifenden ermöglicht es, die durchgeführten Aktionen besser verstehen zu können. Han&Dongre (2014) gliedern die Motive der Angreifer in drei Kategorien.

Politische Motivation:

- Zerstörung, Störung
- Spionage
- Vergeltungsaktionen

Wirtschaftliche Motivation:

- Diebstahl von geistigem Eigentum
- andere Vermögenswerte

Soziokulturelle Motivation:

- Angriffe aus Spaß oder Neugierde
- Wunsch nach Publicity
- Befriedigung des Egos

2.5 Psychologische Grundlagen und Taktiken

Erfolgreiche Social Engineers müssen die unterschiedlichen psychologischen Grundlagen und Anwendungsmethoden, um Menschen zu beeinflussen und in eine bestimmte Richtung lenken zu können, einwandfrei beherrschen. Viele Vorgehensweisen und Techniken sind ausgesprochen effektiv und werden oft von gut ausgebildeten Agentinnen und Agenten meisterhaft eingesetzt (Hadnagy, 2011, S. 240).

Wittenberg (2013) beschreibt die Methoden zur Manipulation der Menschen und gliedert die einzelnen Praktiken anhand soziopsychologischer Forschungen in situationsbezogene Teile, die einzeln genutzt oder miteinander verknüpft werden können. In diesem Abschnitt werden einige der in der Literatur erforschten psychologischen Grundlagen und Taktiken erläutert.

Reziprozität: Diese Methodik basiert auf der Regel der Wechselseitigkeit. Wenn eine Person einer anderen etwas schenkt oder einen Gefallen erweist, erwartet Ersterer, dass dieser Gefallen irgendwann erwidert wird. Diese Grundregel ist tief in den Menschen verankert und deshalb sehr machtvoll.

Man möchte ja nicht als geizig und unverschämt angesehen werden. Social Engineers nutzen diese Methode, um eine Beziehung mit ihren Zielpersonen aufzubauen, indem sie geschickt ein hochentwickeltes, exakt geplantes System der Reziprozität einzusetzen, um an Gegenleistungen gelangen und somit eine Form der Abhängigkeit zwischen den beiden zu schaffen.

Commitment (Verpflichtung) und Konsistenz: Menschen neigen dazu, eine bereits getroffene Entscheidung nicht gerne zurückzuziehen. Intra- und interpsychische Vorgänge treiben uns an, konsistent zu bleiben und uns somit behaglicher zu fühlen. Beim Social Engineering versucht der Angreifer sein Opfer zu einem Commitment zu binden. In der Sozialpsychologie und im Marketing wird dieses Phänomen als „Fuß in der Tür Taktik" bezeichnet. Verkäuferinnen und Verkäufer beginnen Gespräche mit potenziellen Kunden, indem sie eine ganze Reihe von Verpflichtungen setzen. Sie fragen den Kunden beispielsweise, ob es ihm gut gehe.

Einige Beauftragte von Tierschutzorganisationen nutzen diese Taktik sehr eindrucksvoll, indem sie das Gespräch mit dem Satz „Mögen sie Tiere?" beginnen. Nachdem die meisten diese Frage mit „ja" beantworten, lässt sich diese Entscheidung nur schwer zurückziehen. Social Engineers nutzen diese Taktik und arbeiten sich so behutsam Schritt für Schritt vor.

Verstärkt wird ein Commitment, wenn das Versprechen in der Öffentlichkeit vor anderen Menschen verkündet wird (S. Schumacher, 2014). Sitte und Moral sowie die Einhaltung von Verträgen oder Gesetzen zwingen die Opfer verhältnismäßig oft zum gewünschten Handeln (Hadnagy, 2011, S. 244).

Soziale Bewährtheit: Dieses Prinzip nutzt das Verhalten anderer Menschen. Für gewöhnlich nehmen Menschen Reaktionen anderer als valide Entscheidung war, was zu einer Nachahmung führt. Diese Taktik wird ebenfalls im Marketing eingesetzt. In der Werbung wir immer das beliebteste oder bekannteste Produkt präsentiert. Verkäufer können ihre Käuferschaft eingrenzen und genau eine gewünschte Zielgruppe anvisieren, die sich dadurch angesprochen fühlt. Auch wenn sich andere Menschen in einer besonderen Situation unsicher fühlen, wird eine Orientierungslosigkeit übertragen.

Dieses Verhalten wurde bereits in vielen Versuchen, aber auch in der Realität beobachtet, indem Menschen in einer Extremsituation, wie etwa bei einem Unfall oder einem Gewaltverbrechen, das Verhalten der anderen nachahmen und nach Hinweisen für richtiges Verhalten suchen, sei es Hilfestellung anzubieten oder in Ratlosigkeit zu verharren. Angreifende nutzen diese soziale Bewährtheit, um einzelne Auslösemerkmale hervorzurufen, die seine Opfer zu dem beabsichtigen Handeln hinführen (S. Schumacher, 2014).

Sympathie: Sympathie kann als Verstärker aller Überzeugungs- und Täuschungsmechanismen eingesetzt werden. In Bezug auf Social Engineering sucht der Angreifende nach besonderen Eigenschaften, die ihn vertrauenswürdig erscheinen lassen. Das können besondere Eigenschaften oder auch anziehendes und wohlgefälliges Verhalten sein. Social Engineers beobachten und studieren ihre Opfer genau, um die starke Waffe der Sympathie anwenden zu können. Diese Faktoren können Attraktivität, Ähnlichkeit in Bezug auf Aussehen, Alter, Religion, politische Einstellung, oder gemeinsame Interessen sein (S. Schumacher, 2014).

Autorität und Angst: Schon im frühen Kindesalter werden wir dazu erzogen, Autoritätspersonen zu gehorchen. Eltern, Lehrkräfte und Uniformierte werden in unserem Unterbewusstsein automatisch zu Autoritätspersonen zugeordnet. Dies wird durch besonders adrette Kleidung, Luxusgegenstände wie etwa teure Autos und Uhren, aber auch Titel oder Dienstgrade unterstrichen, wie in der Geschichte des Hauptmanns von Köpenick.

Social Engineers nützen diesen Mechanismus, um Menschen damit zu täuschen, dass eine angeblich von der Autorität getroffene Entscheidung automatisch als richtig empfunden wird. Auch die Angst vor drohenden Ereignissen oder vorgesetzten Personen nutzen Social Engineers zu ihren Gunsten.

Oftmals geben sich Social Engineers auch als Systemadministratoren oder Vorstandsmitglieder aus, um Zahlungsanweisungen oder andere Tätigkeiten durchführen zu lassen.

Besonders künstlicher Zeitdruck lässt sich sehr gut mit Angst kombinieren, um durch das Androhen von Konsequenzen Menschen zu unüberlegten Handlungen zu drängen (Hadnagy, 2011; Saurugg, 2007).

2.6 Klassifizierung der Angriffe

Ein Ansatz für die Klassifizierung von Social Engineering Angriffen wird von Foozy et al. (2012) beschrieben. In dieser Forschungsarbeit wird erläutert, dass vor 2006 in der Forschung die unterschiedlichen Angriffe und Bedrohungen der Informationssicherheit in zwei Gruppen unterteilt wurden, und zwar in technische Hackerangriffe und in Social Engineering Angriffe. Neuere Forschungen ab dem Jahr 2006 dokumentierten, dass zwei Arten von Social Engineering Angriffen unterschieden werden können (Foozy et al., 2012).

Menschenbasierende Social Engineering Angriffe: Bei diesen Angriffen werden Methoden verwendet, die eine Interaktion von Angesicht zu Angesicht voraussetzen. Bei dieser Form der Kommunikation kann der Angreifende Informationen über seine Opfer durch die persönliche Interaktion sammeln. Er nutzt dabei die psychologischen Grundlagen wie etwa Angst oder Vertrauen, um durch geschickte Manipulation der Menschen sein Ziel zu erreichen.

Technologiebasierende Social Engineering Angriffe: Diese Art von Social Engineering basiert auf den eingesetzten Technologien zur Erreichung der Ziele. (Maan & Sharma, 2012).

In Kapitel 3.3 werden die unterschiedlichen Angriffe diskutiert.

2.7 Angriffszyklen

In der Forschung "A Mitigation and Prevention Model for Social Engineering Based Phishing attacks on Facebook" beschreiben Jamil et al. (2018) die verschiedenen Anriffszyklen eines typischen Social Engineering Angriffes. Abbildung 2.2 zeigt den Prozess eines Angriffes.

In der ersten Phase (Information Gathering) beginnt der Angreifer mit einer Grundlagenrecherche mit Hilfe von Social Engineering Tools in verschiedenen Datenbanken und sammelt so Informationen über mögliche Schwachstellen. Diese Informationen können Hinweise über besondere Vorlieben des Opfers, finanzielle Informationen, Familieninformationen und viele weitere Informationen liefern, die für den Aufbau einer sozialen Beziehung vonnöten sind.

In der nächsten Phase (Developing Relationship) beginnt der Social Engineer mit einer ersten Anbahnung des Zielobjektes.

Dazu nutzt er die zuvor gesammelten Daten, um schließlich im Schwerpunkt des Angriffes (Exploitation Phase) durch Ausnutzen der psychologischen Faktoren des Opfers die gewünschten Handlungen durchführen zu lassen. Dabei handelt es sich meistens um eine heimtückische Tat, wie die Installation einer Schadsoftware oder andere Aktivitäten, die den Angreifenden näher an seine Zielerreichung bringen.

In der Ausführungsphase (Execution Phase) nutzten Angreifende schließlich alle zuvor vorbereitenden Tätigkeiten aus, um die gewünschten Informationen zu erbeuten. Abschließend kann der Social Engineer die Verbindung zum Opfer abbrechen, oder bei Misserfolg den Angriff erneut mit der ersten Phase beginnen (Jamil et al., 2018).

Abbildung 2.2: Angriffszyklen (in Anlehnung an Jamil et al., 2018)

3 Stand des Wissens

In diesem Kapitel werden die für diese Publikation relevanten Forschungsergebnisse aus den Jahren 2015 bis 2021 beschrieben. Es werden die häufigsten Social Engineering Angriffe aus dem Jahr 2020 detailliert betrachtet und aus der Sicht der angreifenden Personen analysiert, indem die verwendeten Strategien, Methoden und Tools erläutert werden.

Um den Themenbezug zum empirischen Teil herstellen zu können, werden bekannte Normen, Best Practice Frameworks und andere Schutzmaßnahmen bzw. Analysen detailliert behandelt.

3.1 Aktueller Stand der Forschung über Häufigkeit der Überzeugungsprinzipien

Bulee et. al (2017) untersuchten in ihrer Studie, inwiefern die verschiedenen psychologischen Grundlagen und Überzeugungsprinzipien (Kapitel 2.5) in erfolgreichen Social Engineering Angriffen eingesetzt werden können. Dafür wurden insgesamt 74 von Social Engineers geschriebene Szenarien ausgewertet, indem die Angriffe in einzelne Schritte zerlegt wurden, um die verwendeten Prinzipien zu identifizieren. Es wurden in den betrachteten 74 Szenarien 142 Angriffsschritte ermittelt.

Der Studie zufolge ist Autorität das Prinzip mit der stärksten Wirkung. Es wurde bei mehr als der Hälfte (63 %) aller untersuchten Angriffe eingesetzt. Des Weiteren wurde in der Studie festgestellt, dass die Unterscheidung, ob der Angriff über das Telefon oder persönlich stattgefunden hat, starken Einfluss auf die Ausführung und die Auswahl der Überzeugungsprinzipien hat, wobei bei den meisten Szenarien mehrere Prinzipien gestaffelt eingesetzt wurden.

Die nachfolgende Abbildung 3.1 zeigt eine grafische Darstellung der identifizierten Prinzipien mit ihren Häufigkeiten. Hier wird demonstriert, dass Autorität mit großem Abstand (63,3 %) gegenüber Sympathie (13,3 %) und Reziprozität (11,1 %) sowie Commitment (10,6 %) in den Angriffen eingesetzt wird. Die Prinzipien Übereinstimmung und Angst wurden nur bei sehr wenigen Angriffen herangezogen (Bullée et al., 2018).

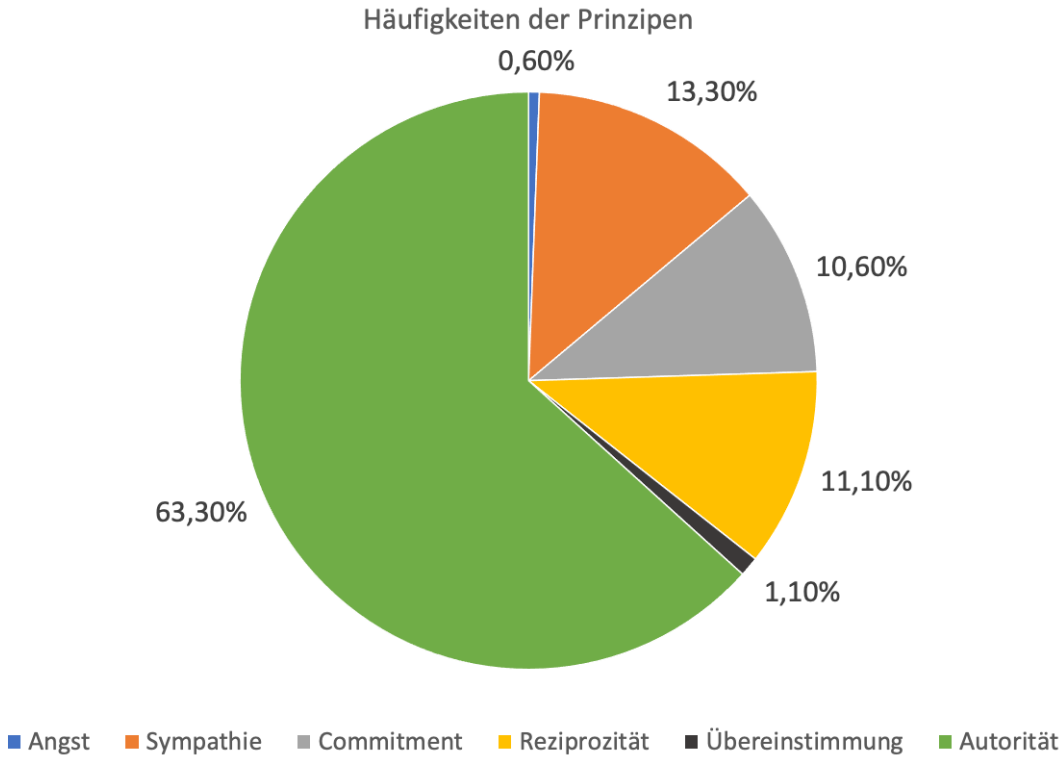

Abbildung 3.1: Häufigkeiten der Prinzipien (in Anlehnung an Bullée et al., 2018)

Eine Studie des amerikanischen Telekommunikationskonzernes Verizon (2020) beschreibt in dessen jährlichen Bericht über Datenschutzverletzungen, dass 22 % aller erfolgreichen und bestätigten Datendiebstähle mithilfe von Social Engineering durchgeführt wurden. Weiters wurde in der Studie erhoben, dass etwa 90 % der Social Engineering Angriffe auf die

Angriffsmethode Phishing und Pretexting (15 %) (Kapitel 3.3) zurückzuführen sind. Die anderen Methoden lagen in der Studie statistisch nicht relevant bei etwas mehr als 3 %.

Besonders beachtenswert für weitere Forschungen ist die Gegebenheit, dass laut Verizon 96 % der Attacken via E-Mail erfolgten, während jedoch nur 3 % aller Angriffe über Webseiten durchgeführt wurden. Nur 1 % aller Datendiebstähle geschah über das Medium Telefon bzw. SMS. Die am häufigsten kompromittierten Datentypen waren Zugangsinformationen (VERIZON Data Breach Investigations Report 2020, 2020).

3.2 Penetrationstests – Forschungsergebnisse

Im Zuge einer Militärübung der NATO wurden Soldatinnen und Soldaten aus vielen verschiedenen Nationen von einer Forschungsgruppe des NATO Strategic Centre of Excellence durch Social Engineering getäuscht und demonstrierten so die besondere Effektivität dieser Angriffsart durch den Einsatz von Social-Media-Kanälen. Mehrere Wochen lang erstellten die Penetrationstester gefälschte Seiten und Profile von Militärangehörigen sowie diversen geschlossenen Gruppen auf Social-Media-Kanälen mit Bezug zu der im gleichen Zeitraum abgehaltenen Militärübung.

Durch gezielte Werbung auf Facebook konnten die Forscher innerhalb des Zeitraumes von vier Wochen etwa 150 Soldaten eindeutig identifizieren und zudem viele Daten und Informationen erbeuten. Unter diesen Daten waren auch viele sensible und klassifizierte Informationen über Truppenbewegungen und Standorte von Einheiten. Zusätzlich erschlichen die Forscher sehr private Informationen über Familienstand und Nutzung von Dating Applikationen. Die Forscher konnten außerdem einzelne an der Übung teilnehmende Soldatinnen und Soldaten zu unerwünschten Taten, wie etwa zum bewussten Verlassen des befohlenen Standortes zwingen.

Aus diesen Penetrationstests konnte von der Forschungsgruppe abgeleitet werden, dass Angreiferinnen und Angreifer durch die beträchtliche Menge an gewonnenen persönlichen Daten die gewünschte Zielgruppe von Soldatinnen und Soldaten so beeinflussen können, um unzulässiges Handeln zu erzwingen (Field, 2019; Schneier, 2019).

3.3 Häufigste Social Engineering Angriffe

In diesem Unterkapitel werden die häufigsten Social Engineering Angriffe aufgezählt und beschrieben. Ein Grundverständnis für die einzelnen Angriffe ist Voraussetzung für die Ausarbeitung einer Handlungsempfehlung.

Die vom Sicherheitsunternehmen Infosec (2020) aufgelisteten Ergebnisse der häufigsten Social Engineering Angriffe im Jahr 2020 decken sich mit anderen aktuellen Studien (Pagani, 2020).

- Phishing
- Wateringhole
- Pretexting
- Baiting and quid pro quo attacks
- Tailgating

3.3.1 Phishing

Phishing gehört zu den am verbreitetsten Social Engineering Angriffen und zählt laut Verizon (2020) zu der am häufigsten eingesetzten Angriffsart bei bestätigten Datenschutzverletzungen (Bisson, 2019; Gupta et al., 2016; VERIZON Data Breach Investigations Report 2020, 2020). Der Name entstammt aus dem englischen Wort für fischen „fisching" und Passwort. Daraus abgeleitet entwickelte sich „Phishing" (Passwort-fischen) (Möhring, 2020).

Durch geschickte Täuschung mit Unterstützung von diversen technischen Hilfsmitteln versuchen angreifende Personen an private und vertrauliche Daten zu gelangen, wie etwa Namen, Adressen, Passwörter oder Bankdaten, indem sie die Absenderin bzw. Absender oder den Link seriös erscheinen lassen. Dabei wird durch den Einsatz von verschiedenen psychologischen Grundlagen die Irreführung verstärkt.

Die Angreiferinnen und Angreifer nutzen dabei Drohungen, Neugierde, Angst oder auch Dringlichkeit, um das Opfer zu der gewünschten Handlung zu zwingen.

Die technischen Hilfsmittel werden nach Beurteilung des geeigneten Übertragungsmediums ausgewählt. Oft werden diese Angriffe mithilfe von E-Mails umgesetzt (Gupta et al., 2016). Laut dem jährlichen Phishing Report von Enisa (2020) wurden im vierten Quartal 2019 über 74 % der Phishing Angriffe mit Web-Seiten, die HTTPS[5] Zertifizierungen unterstützen, erfolgreich umgesetzt.

Verbreitete Maßnahmen zur Minimierung von Phishing Angriffen sind Sicherheitsschulungen. Zusätzlich zu den Schulungen kommen technische Abwehrmaßnahmen zum Einsatz, die E-Mails von betrügerischen Absenderinnen und Absendern filtern und blockieren (ENISA ETL Report 2020 - Phishing (EN), 2020).

Einer Studie des Sicherheitsunternehmens Proofpoint (2020) zufolge führen 95 % der befragten Unternehmen Sicherheitsschulungen durch. Jedoch handelt es sich bei 30 % um keine modulartig aufgebauten sowie nicht zielorientierten, auf alle Anwenderinnen und Anwender ausgerichteten Schulungen. Etwa ein Drittel der Userinnen und User, die eine simulierte Phishing E-Mail bekamen, waren dazu geneigt, auf die Aufforderungen in der E-Mail einzugehen (State of the Phish 2020, 2020).

Um die Verwundbarkeit des eigenen Unternehmens zu testen, sendete der Domainanbieter GoDaddy nach der unternehmensweiten Sicherheitsschulung einen simulierten Phishing Angriff via E-Mail an die eigenen Mitarbeiterinnen und Mitarbeiter. Um den vermeintlichen Weihnachtsbonus zu bekommen, bestätigten etwa 500 Mitarbeiter den angeblichen Link. (Domainanbieter gaukelte Mitarbeitern Weihnachtsbonus vor und warnte dann vor Phishing, 2020).

Prognosen zeigen, dass das Übertragungsmedium der Phishing Angriffe, von Social Media Messaging und künstlicher Intelligenz, den Einsatz von E-Mails ablösen wird. Mit Phishing-as-a-Service (PhaaS) können technisch wenig versierte Personen gegen eine Gebühr Phishing Angriffe von Anbietern durchführen lassen (ENISA ETL Report 2020 - Phishing (EN), 2020; State of the Phish 2020, 2020).

[5] Hypertext Transfer Protocol Secure (HTTPS) steht für ein sicheres Übertragungsprotokoll

Phishing kann in mehrere Kategorien unterteilt werden. Salahdine & Kaabouch (2019) klassifizierten die Phishing Angriffe in fünf Unterkategorien (Salahdine & Kaabouch, 2019). Abbildung 3.2 zeigt eine Darstellung der weiteren Kategorien von Phishing.

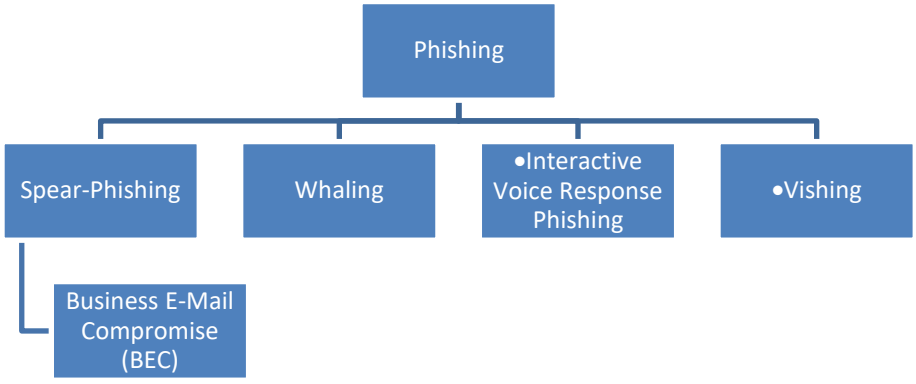

Abbildung 3.2: Kategorien von Phishing (in Anlehnung an Salahdine & Kaabouch, 2019)

- Spear-Phishing:

Eine gezielte Form des Phishings ist das sogenannte Spear (Speer)-Phishing. Durch Recherche oder Beobachtung wird das Ziel ausgewählt und so viel Informationen wie möglich gesammelt. Der Angriff wird mit Hilfe der angehäuften Ergebnisse so vorbereitet, dass er für das Opfer authentisch wirkt, wodurch er erfolgsversprechend ist (Phishing Activity Trends Report, 2020; Phishing ENISA Threat Landscape, 2020).

- Business E-Mail Compromise (BEC):

Ähnlich wie beim Spear-Phishing werden bei dieser Betrugsmasche gezielt Einzelpersonen, aber auch ganze Unternehmen ausgewählt und durch Social Engineering betrogen.

Der wesentliche Unterschied liegt dabei aber in der Durchführung von legitimen Überweisungsanfragen durch geschickte Täuschung, um so unautorisiert Geldtransfers durchführen zu können.

Manchmal werden auch geschäftliche E-Mail Accounts kompromittiert und dadurch diverse personenbezogene Daten von Mitarbeiterinnen und Mitarbeitern widerrechtlich erbeutet. Diese werden für missbräuchliche Tätigkeiten, wie etwa Geldauszahlungen bei Steuererklärungen, verwendet.

Das FBI berichtet von über 166 000 gemeldeten internationalen Vorfällen von BEC im Zeitraum zwischen 2016 und 2019. Dabei sollen 26 Milliarden USD erbeutet worden sein (Internet Crime Complaint Center (IC3) | Business Email Compromise The $26 Billion Scam, 2019).

- Whaling:

Diese Methode beschreibt den Angriff auf hochrangige Führungskräfte, um vertrauliche Daten oder Geld zu ergaunern. Dabei werden verschiedene Angriffsvektoren wie E-Mail oder URL-Spoofing[6] angewendet (Was ist ein Whaling-Angriff?, 2021).

- Interactive Voice Response Phishing:

Der Angreifende täuscht seine Opfer durch das Medium Telefon und gibt sich als eine andere Person aus (Anand, 2019).

- Vishing:

Diese Methode ähnelt dem Phishing und setzt oft in einem Bereich an, in dem Phishing nicht mehr wirksam ist. Dabei werden die Opfer mündlich (meistens über das Telefon) zu den erwünschten Handlungen gezwungen.

[6] Beim URL-Spoofing wird die tatsächliche Andresse der Webseite verschleiert

Sehr oft meldet sich das Opfer bei dem „vermeintlichen“ hilfsbereiten Techniker, nachdem eine Warnmeldung durch eine infizierte Webseite versendet wurde. Gegen Bezahlung löst der Techniker das von ihm selbst verursachte Problem (Was ist Vishing?, 2021).

3.3.2 Wateringhole

Bei dieser Form des Angriffes werden Webseiten gezielt durch Schadsoftware infiziert. Sobald jemand eine der Webseiten besucht, wird ein Download ausgelöst, welcher den Rechner oder das Netzwerk des Users kompromittiert (Cyber Defence News, 2020). Besonders effektiv wird die Form des Angriffes mit Phishing verknüpft, indem die Zielpersonen zu den Webseiten geleitet werden (Watering Hole - Website Attacke | Proofpoint DE, 2016).

3.3.3 Pretexting

Pretexting entspringt aus dem englischen Wort "pretext" und bedeutet auf Deutsch "Vorwand". Durch gezielt ausgewählte psychologische Grundlagen zur Beeinflussung von Menschen (Kapitel 2.5) erfindet der Social Engineer einen bestimmten Vorwand, um bei dem ausgewählten Opfer ein gewisses Gefühl oder eine Charaktereigenschaft hervorzurufen und den Verstand zu täuschen. Sehr oft wird dabei die Hilfsbereitschaft oder Gutgläubigkeit ausgenutzt.

Die Täter nutzen Soziale Netzwerke und das Internet für die notwendigen Personenrecherchen und planen so den Angriffsablauf (Böhl, 2020).

Ein Beispiel eines Pretexting Angriffes ist der sogenannte Enkeltrick, bei dem besonders Senioren ausgetrickst werden. Es wird unter vorgetäuschter Familienzugehörigkeit an die Hilfsbereitschaft appelliert, bis sich das Opfer dazu bereit erklärt, den gewünschten Geldbetrag zu überweisen (Grass, 2015).

3.3.4 Baiting and quid pro quo attacks

Ähnlich wie beim Phishing werden die Opfer mit bestimmten Methoden geködert, um etwa an Zugangsdaten oder andere Informationen zu gelangen bzw. Computer oder Netzwerke zu infizieren. Dabei werden nicht nur Online-Methoden angewendet. Bei einer quid pro quo Attacke wird grundsätzlich das Prinzip der Gegenleistung zum Einsatz gebracht, indem wie beim Baiting Informationen oder besondere Dienstleistungen vom Social Engineer versprochen werden (Bisson, 2019).

3.3.5 Tailgaiting

Beim Tailgaiting oder Piggybacking (Huckepack) folgt der Social Engineer einer anderen Person unautorisiert in einen geschützten Bereich. Der Angreifende kann sich als Servicetechnikerin bzw. Servicetechniker ausgeben, um Zugang zu den gewünschten Räumlichkeiten zu bekommen. Oft genügt es aber auch den vermeintlichen Kollegen darum zu bitten, die Türe aufzuhalten. Ein Sicherheitsberater berichtete, im Rahmen eines Penetrationstests mit dieser Methode Zugang zu mehreren Stockwerken und sogar zum Archiv eines großen Finanzdienstleisters erhalten zu haben (Bisson, 2019).

3.4 Social Engineering Angriff Framework

Mouton et.al (2016) haben in ihrer Forschung detaillierte Angriffsvorlagen abgeleitet, indem sie reale Angriffe verallgemeinerten und im Rahmen eines Social Engineering-Attack-Framework (SEAF) abbildeten. Dieses Framework ermöglicht weiterführende Studien für die Entwicklung von Awarenessmaßnahmen.

Das Framework basiert auf den von Mouton et.al in vorherigen Studien entwickelten Modellen und verwendet sieben Bausteine und sechs Phasen (Mouton et al., 2016).

Folgende Bausteine zur Angriffsdurchführung werden in dem Framework definiert:

- Kommunikation: Direkte Kommunikation (Bidirektional und Unidirektional) oder indirekte Kommunikation.
- Social Engineer: Kann eine Einzelperson oder eine Gruppe bzw. eine Organisation sein.
- Ziel: Einzelperson oder Organisation (Unternehmen).
- Medium: Methode der Kommunikationsübertragung.
- Motivation des Angriffes: Etwa finanzielle Interessen oder wie in Kapitel 2.4 beschriebe Interessen.
- Compliance Prinzipien: Psychologische Grundlagen der Täuschung (Kapitel 2.5).
- Technik: Jene Methoden, die eingesetzt werden, um das Ziel zu erreichen.

Nachfolgend werden die von Mouton et al. (2016) beschriebenen Phasen in der notwendigen Reihenfolge aufgelistet:

1. Angriffsformulierung: Identifikation des Zieles und der Motivation.
2. Sammeln von Informationen: Die Informationen werden aus verschiedenen Quellen identifiziert, gesammelt und anschließend bewertet.
3. Vorbereitung: Hier werden die gesammelten Daten miteinander kombiniert und analysiert. Danach werden Angriffsvektoren definiert.
4. Beziehung aufbauen: Geplante Kommunikation aufbauen und Vertrauen herstellen.
5. Beziehung ausnutzen: Gewünschte Aktionen vom Opfer ausführen lassen.

6. Reflexion: Wenn die gewünschten Ziele erreicht wurden, kann der Angriff abgeschlossen werden. Der Angriff fängt wieder von vorne mit der ersten Phase an, falls die Ziele nicht erreicht werden konnten.

3.5 Frameworks für Schutz- und Schulungsmaßnahmen

3.5.1 Higher Education Awareness Lifecycle Model

Auf der Grundlage des von Mouton et.al (2016) beschriebenen Frameworks (Kapitel 3.4) wurde von Nguyen & Bhatia (2020) ein Modell entwickelt, indem neun Angriffe auf eine Hochschuleinrichtung und ihre Mitarbeiterinnen und Mitarbeiter sowie Studierenden abgebildet wurden. Die Autorinnen und Autoren konnten aufgrund der Angriffszenarien ein Framework für ein Awareness-System erzeugen. Die nachfolgende Abbildung 3.3 illustriert das erstellte Framework für Schutzmaßnahmen (Nguyen & Bhatia, 2020).

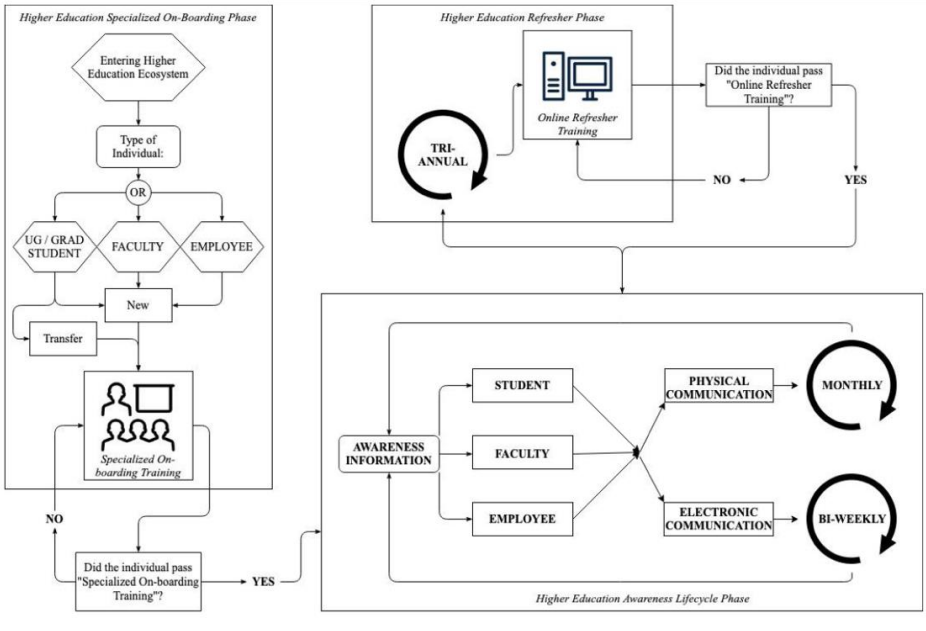

Abbildung 3.3: Higher Education Awareness Lifecycle Model (Nguyen & Bhatia, 2020

Das System beschreibt einen Lebenszyklus für ein Social Engineering Schulungsprogramm. Alle Angestellten, Lektorat und Studierende nehmen an einem bestimmten Trainingsprogramm teil, welches positiv abgeschlossen werden muss. Nach erfolgter Absolvierung dieses Grundlehrganges werden alle Schulungsteilnehmerinnen und Schulungsteilnehmer iterativ in bestimmten zeitlichen Abfolgen durch Informationen in Bezug auf Sicherheitsmaßnahmen über verschiedene Medien informiert. Ein Drei-Jahres Zeitplan umfasst auch ein Online-Schulungsprogramm, welches ebenso positiv absolviert werden muss (Nguyen & Bhatia, 2020).

3.5.2 Social Engineering Defence Model

Ein nachhaltiges Modell von Social Engineering Abwehrmaßnahmen beschreibt Quinlan (2020). In dem theoretischen Modell wurden mehrere Forschungsansätze zusammengefasst und miteinander kombiniert. Daraus resultierte ein Trainingsprogramm, welches aus vier Phasen besteht. Abbildung 3.4 illustriert die vier iterativen Phasen des „Social Engineering Defence Models".

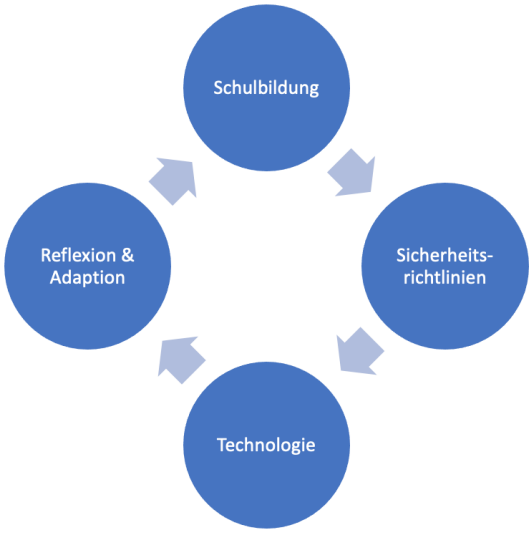

Abbildung 3.4: Social Engineering Defence Model (in Anlehnung an (Quinlan, 2020)

In der ersten Phase (Schulbildung) wird erläutert, dass Schulungen für die Informationssicherheit bereits in das Grundschulsystem integriert werden sollten. Durch diverse Programme sowie interaktive Videospiele könne man den zukünftigen Arbeitskräften bereits in der Kindheit an die Gefahren von Social Engineering näherbringen, um Angriffe besser erkennen und darauf reagieren zu können (Quinlan, 2020). Ein deutsches Start-Up veröffentlichte 2021 das Programm "Fuchs im Netz". Es ermöglicht Kinder ab sieben Jahren, spielerisch den Umgang mit Informationssicherheit und den Gefahren im Internet kennenlernen (Datenschutz, 2021).

Die darauffolgende Phase (Sicherheitsrichtlinien) beschreibt ein System aus mehreren Schichten, die wie eine Checkliste von Sicherheitsverantwortlichen zu beurteilen sind. Die erste Schicht besteht aus den zu schützenden Daten des Unternehmens. Die weiteren Schichten werden aus technischen sowie organisatorischen Maßnahmen gebildet, die es angreifenden Personen erschweren, an die Daten zu kommen. Die letzte Schicht ist üblicherweise die Schnittstelle des internen Firmennetzwerkes nach außen.

Phase drei (Technologie) fokussiert auf technologische Hilfsmittel, die Social Engineering Angriffe erkennen können. Diverse Anbieter bieten dazu Programme und Tools an, die Phishing E-Mails erkennen und als verdächtig einstufen können. Durch Einsatz von künstlicher Intelligenz könne dazu ein effektives Werkzeug zur Identifikation von Social Engineering Angriffen eingesetzt werden, meint Quinlan (2020).

In der letzten Phase (Reflexion & Adaption) werden Angriffe in ihre Bestandteile zerlegt und evaluiert, wie daraus Schutzmaßnahmen im Unternehmen implementiert werden können (Quinlan, 2020).

3.5.3 Social Engineering Compliance

Alharthi & Regan (2021) betrachten in ihrer Studie Social Engineering Sicherheitsrichtlinien in Unternehmen. Auf Grundlage vorangegangener Studien und einer breit gefächerten, repräsentativen Umfrage mit 1523 Teilnehmerinnen und Teilnehmern, entwickelten Alharthi & Regan ein Framework für Unternehmen.

Dazu wurden zuerst vier Social Engineering Angriffsziele definiert:

- Menschen (People)
- Daten (Data)
- Soft/Hardware
- Netzwerk (Network)

Aufgrund der Umfrageergebnisse und Berücksichtigung der Schutzziele (Kapitel 2.2), wurden 18 formale Social Engineering Sicherheitsrichtlinien konkretisiert, die in Abbildung 3.5 dargestellt werden. Die Richtlinien umfassen sowohl technische als auch organisatorische Schutzmaßnahmen (Alharthi & Regan, 2021).

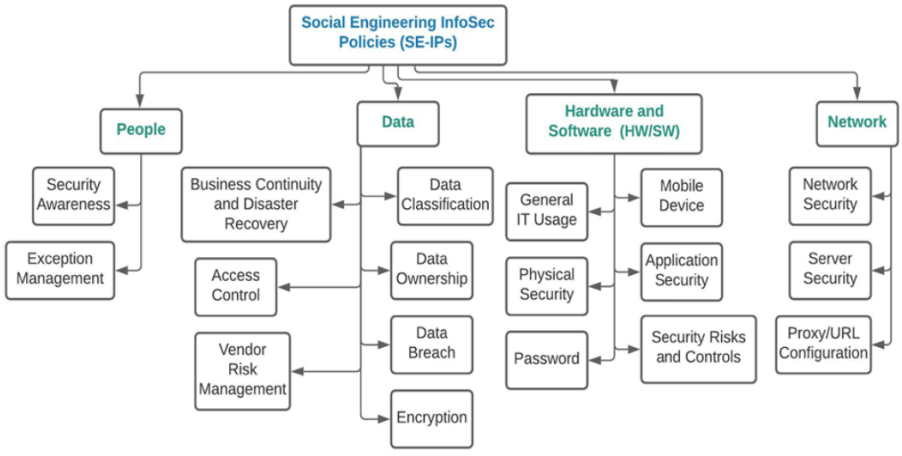

Abbildung 3.5: Social Engineering Sicherheitsrichtlinien (Alharthi & Regan, 2021)

Im Zuge der Umfrage wurde festgestellt, dass nur 51,18 % der identifizierten Social Engineering Sicherheitsrichtlinien in den Unternehmen implementiert wurden.

Besonders interessant ist die Auswertung der Umfrageergebnisse durch eine Clusteranalyse der Unternehmen im öffentlichen und privaten Sektor.

Hier zeigen die Ergebnisse, dass die Einbindung von Sicherheitsrichtlinien im
privaten Sektor höher ist als in staatlichen Organisationen (Alharthi & Regan, 2021).

3.5.4 Employee Security Index

In ihrer Publikation haben Franz & Benlian (2020) in einem Feldexperiment mit simulierten Phishing Angriffen die Wirksamkeit einer Kennzahl für das Sicherheitsbewusstsein der Belegschaft „Employee Security Index" (ESI) untersucht.

Für die Simulation wurden je nach Vorbereitungszeit und Aufwand durch Betrachtung der Angreiferinnen und Angreifer mehrere Kategorien von Angriffs-Komplexitäten definiert und demnach drei verschiedene Phishing Szenarien erstellt. Das für das Feldexperiment benötigte Schulungsprogramm beinhaltet drei Phasen:

- Präsenzschulung:

  Jeder Angestellte absolvierte eine 90-minütige Präsenzschulung mit verschiedenen Themenbereichen von Social Engineering und Cybersicherheit. Zudem wurden bekannte Sicherheitsvorfälle vorgeführt und nachbesprochen.

- E-Learning:

  Die in der Präsenzschulung präsentierten Inhalte wurden in ein E-Learning System integriert und unternehmensweit eingesetzt.

- Lernmoment durch die Simulation:

  Der erwünschte Lern-Effekt sollte durch das Gefühl erzeugt werden, selbst Opfer eines Angriffes geworden zu sein.

Durch das Öffnen eines gefälschten Links oder das Herunterladen einer Schadsoftware im Zuge der Angriffssimulation wurden die Teilnehmer unmittelbar nach dem Fehlverhalten zu einer interaktiven Erklärung der Schutzmaßnahmen weitergeleitet.

Das Feldexperiment erstreckte sich innerhalb eines Zeitraumes von etwa sechs Monaten. Der Schwierigkeitsgrad der simulierten Angriffe erhöhte sich stetig.

Das Framework ESI besteht aus Kennzahlen einer Skala von 0 bis 100, um das Sicherheitsverhalten messbar zu machen und um ein standardisiertes Verfahren zur Interpretation der Werte definieren zu können. Abbildung 3.6 (nächste Seite) zeigt die Bewertungsskala.

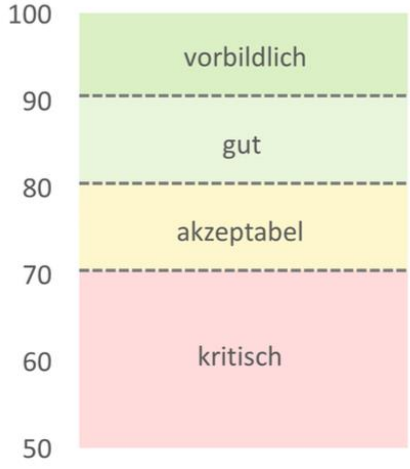

Abbildung 3.6: Bewertungsskala ESI (Franz, 2020)

Durch die Klickrate in der Simulation wurden die Werte berechnet, wobei der Startwert zu Beginn des Experiments bei 44 lag. Die Kennzahl wurde unternehmensweit auf den Wert von 89 erhöht und somit die signifikante Wirksamkeit von kennzahlenbasierenden Schutzmaßnahmen bewiesen (Franz & Benlian, 2020).

3.6 Social Engineering Tools

Die geschickte Täuschung von Menschen wird durch die psychologischen Grundlagen umgesetzt. Die Kombination von Täuschung mit technischen Tools, welche die bereits vorgefertigten Angriffsvektoren integrieren, erleichtert angreifenden Personen, aber auch Penetrationstestern, die Vorbereitung und Abwicklung der Angriffe.

Viele der Toolkits basieren auf Open-Source-Produkten und werden zur Unterstützung von Penetrationstests entwickelt, um Security Fachleuten die Möglichkeit zu bieten, ihre eigenen Systeme bzw. Netzwerke auf Schwachstellen zu testen. Selbstverständlich werden die sehr umfangreich gestalteten Programme auch für kriminelle Zwecke genutzt (Franz & Benlian, 2020).

3.6.1 Social Engineering Toolkit

Eine oft gebrauchte Sammlung von Tools ist das Social Engineering Toolkit (SET), welches frei verfügbar auf verschiedenen Betriebssystemen integrierbar ist. Das auf dem Linux Betriebssystem "Kali-Linux" vorinstallierte Programm bietet ein umfassendes Framework für viele verschiedene Angriffsvektoren.

Die nachfolgende Abbildung 3.7 zeigt das Hauptmenü von SET. Es bietet verschiedene Angriffswege, wie Spear-Phishing, Phishing, Schadsoftware und andere integrierte Angriffe (Beckers et al., 2017; Chapple & Seidl, 2019).

Zur Illustrierung der einfachen Bedienung ohne besondere technische Grundlagenkenntnisse, wird ein vom Autor erstellter simulierter Phishing Angriff (im eigenen Netzwerk) erstellt. Ziel dieses Angriffes ist das Erbeuten von Passwörtern durch eine gefälschte Webseite.

Abbildung 3.7: SET Hauptmenü (eigene Darstellung)

Die nachfolgende Abbildung 3.8 zeigt das Eingabefeld (2) für die Auswahl der geklonten Webseite und die IP-Adresse des Netzwerkes (1), auf welcher die gefälschte Webseite betrieben wird

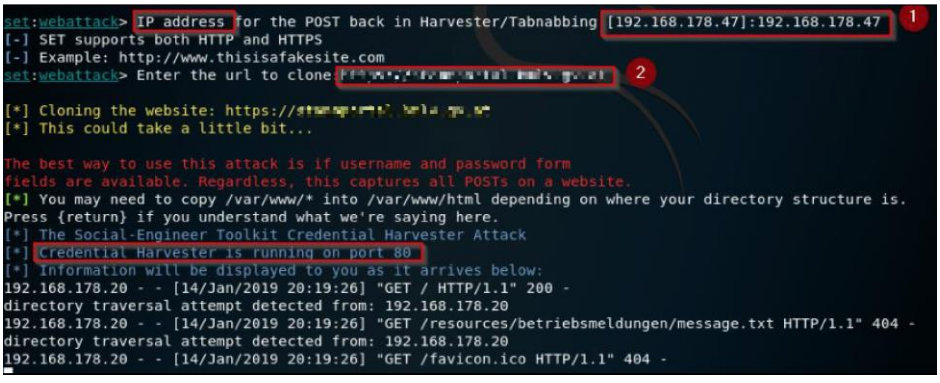

Abbildung 3.8: SET Hauptmenü (eigene Darstellung)

Die URL[7] der Webseite kann via E-Mail oder mit anderen Übertragungsmedien versendet werden. Anschließend wird nur noch gewartet, ob jemand den Link öffnet und seine Zugangsdaten eingibt. Nachdem der User seine Zugangsdaten in die Eingabemaske eingegeben hat, bekommt der Social Engineer automatisch die Zugangsinformationen (Benutzername und Passwort) im Klartext zugesendet (Abbildung 3.9).

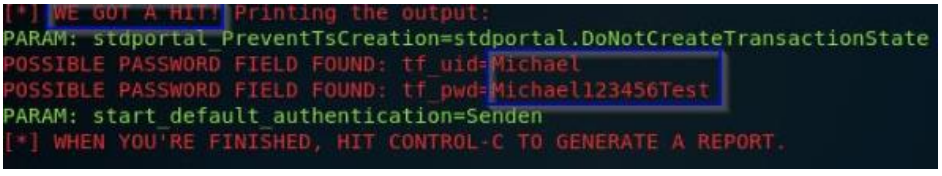

Abbildung 3.9: Zugangsdaten der geklonten Webseite (eigene Darstellung)

3.6.2 Maltego

Das ebenfalls auf dem Betriebssystem "Kali Linux" verfügbare Tool "Maltego" ermöglicht den Benutzerinnen und Benutzern alle E-Mail-Adressen eines Unternehmens automatisiert im Internet zu suchen. Somit können Phishing oder gezielte Spear-Phishing Nachrichten versendet werden.

Zusätzlich unterstützt das Tool die Suche nach Metadaten[8] der Unternehmen. Die gesammelten Informationen über Personen und Daten können grafisch für die Analysen von Netzwerken (Abbildung 3.10) ausgewertet werden, um Attackierenden mögliche Ausgangspunkte und Entitäten für verschiedene Angriffsvektoren bereitzustellen (Beckers et al., 2017; Ries, 2013).

[7] URL - Uniform Resource Locator, ist die Adresse einer einzelnen Webseite
[8] Strukturierte Daten über Informationsressourcen

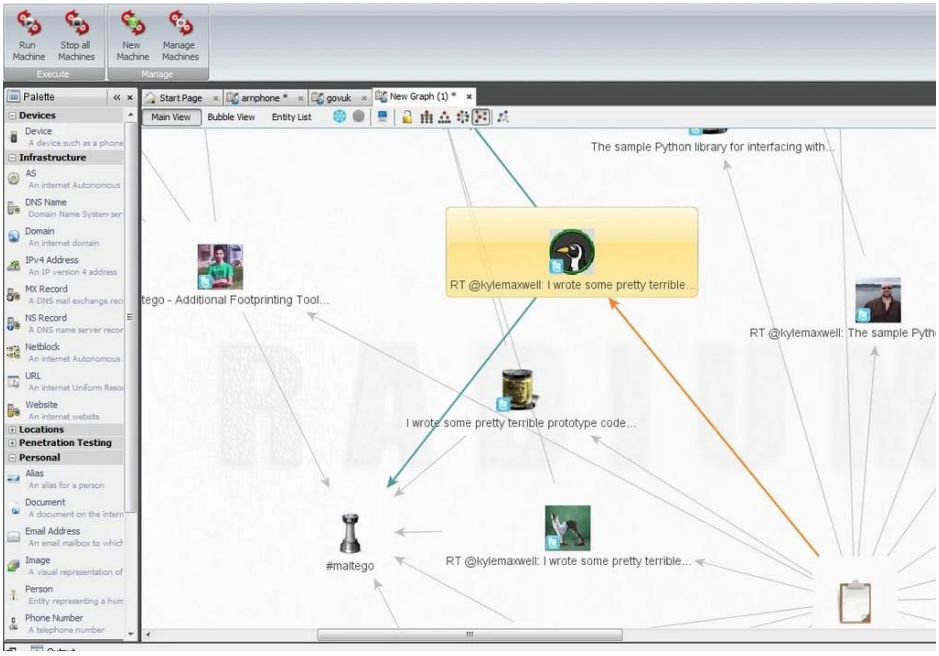

Abbildung 3.10: Netzwerkanalyse mit Maltego (Beckers et al., 2017; Ries, 2013)

3.7 Tätigkeiten des CISO in Bezug auf Social Engineering

Grundsätzlich ist ein CISO für die Informationssicherheit im Unternehmen verantwortlich. Die Bezeichnung des Chief Information Security Officer beschreibt seine bzw. ihre Funktion und Position im Unternehmen. Im Gegensatz zu diversen Funktionen von Sicherheitsverantwortlichen, sollte ein CISO grundsätzlich der Geschäftsführung unterstellt werden. Er oder sie ist dafür verantwortlich, dass die gesetzlichen und vertraglichen Vorgaben und Compliance[9] Bestimmungen im Unternehmen erstellt und eingehalten werden.

Die Aufgaben des CISO sind branchenspezifisch unterschiedlich, deswegen werden auch je nach Branche und Geschäftsmodell diese angepasst und regelmäßig neu beurteilt (Welche Aufgaben ein CISO übernehmen muss, 2021).

[9] Interne Richtlinien durch Unternehmen und Mitarbeiter

ISO-Standards und viele weitere Normen sowie Frameworks bieten den CISOs Unterstützung bei der Umsetzung von Richtlinien. Sie bieten zusätzlich die Möglichkeit einer Zertifizierung, um gegenüber Behörden, Partnern und Kunden nachweisen zu können, dass es sich um eine Organisation handelt, die alle Maßnahmen zur Optimierung der Informationssicherheit unternimmt (*ISO 27001*, 2021; *Was macht einen CISO aus: Erfolg und Führungsverhalten im Bereich IT-Sicherheit in Unternehmen*, 2018).

Einer Umfrage des Cybersicherheitsunternehmens Kaspersky Lab zufolge (2018) fühlen sich nur etwa 58 % der CISO angemessen in Geschäftsentscheidungen eingebunden, um frühzeitig auf Prozesse und Technologien Einfluss zu nehmen. 26 % aller befragten CISOs sind dauerhaft im Vorstand vertreten und können somit an allen Sitzungen und Entscheidungen aktiv mitwirken. Die große Mehrheit empfindet sich aufgrund der stark zunehmenden Anzahl und der Auswirkungen der Angriffe als zu wenig in strategische Führung eingebunden. Der Einfluss der CISOs in die Line of Business (LOB) wird von den Umfrageteilnehmern als zukünftiger Trend angesehen (Was macht einen CISO aus: Erfolg und Führungsverhalten im Bereich IT-Sicherheit in Unternehmen, 2018).

3.8 Normen und Best Practice

Nationale sowie EU-Gesetze und Verordnungen sind die Basis eines Konzepts für die Informationssicherheit in Unternehmen. Verschiedene Sicherheitsaudits und daraus vergebene Zertifizierungen wie etwa nach ISO/IEC, können für Organisationen sowie deren Partner und Kunden als anerkanntes quantifizierbares Messkriterium für Sicherheit von Informationen stehen und sind wichtige Nachweise, dass staatliche und unternehmensinterne Anforderungen und Richtlinien erfüllt werden.

3.8.1 ISO 27001

Die ISO 27001 Norm spezifiziert die Qualitätsanforderungen eines Informationssicherheitsmanagementsystems (ISMS) und ermöglicht Unternehmen eine Zertifizierung, die häufig von Kundinnen und Kunden oder geschäftlichen Kontakten gefordert wird. Im Anhang A der ISO-Norm werden 114 Sicherheitsmaßnahmen (Controls) in 14 nachfolgenden Kategorien angeführt (BSI IT Grundschutz vs. ISO 27001 - iso-27001.at, 2020; ISO 27001, 2021; Irwin, 2020).

1. Richtlinien zur Informationssicherheit
2. Organisation der Informationssicherheit
3. Personelle Sicherheit
4. Vermögensverwaltung
5. Zugangskontrolle
6. Kryptographie
7. Physische und umgebungsbezogene Sicherheit
8. Betriebssicherheit
9. Kommunikationssicherheit
10. Systembeschaffung, Entwicklung und Wartung
11. Lieferantenbeziehungen
12. Management von Informationssicherheitsvorfällen
13. Aspekte der Informationssicherheit im Business Continuity Management
14. Compliance

Die aufgezählten ISO 27001 Anhang A Kategorien unterstützen bei der Identifikation von Risiken. Der ergänzende Standard 27002 ermöglicht einen detaillierten Überblick über die notwendigen Sicherheitsrichtlinien (Irwin, 2020).

3.8.2 BSI IT-Grundschutz

Ein vom deutschen Bundesamt für Informationssicherheit (BSI) erstellte Katalog für IT-Grundschutz zeigt detaillierte Maßnahmen und Empfehlungen für den Aufbau und Sicherstellung eines ISMS. Der BSI-Grundschutz Katalog ist im Gegensatz zur ISO 27001 Norm kostenlos und ist auf der BSI Webseite frei verfügbar. Zurzeit besteht der Katalog aus vier Teilen und wird von Unternehmen als sehr umfangreich angesehen (BSI - IT-Grundschutz-Standards, 2020; ISO 27001, 2021).

Folgende vier Teile sind mit Stand Februar 2021 verfügbar:

- 200-1: Managementsysteme für Informationssicherheit (vollständig kompatibel zu ISO 27001)
- 200-2: IT-Grundschutz-Methodik
- 200-3: Risikomanagement
- 200-4: Notfallmanagement

Der BSI-Grundschutz ist eher technisch ausgerichtet, während die ISO 27001 Norm auf Geschäftsprozesse ausgelegt ist, dafür aber auf einer sehr abstrakten Ebene angesiedelt und offener formuliert wird (ISO 27001, 2021).

3.8.3 Österreichisches Informationssicherheitshandbuch

Das vom österreichischen Bundeskanzleramt in der Version 4 erstellte kostenlose Handbuch beschreibt wie die ISO 27001 Norm und der BSI-Grundschutzkatalog die Vorgehensweise für die Etablierung eines ISMS.

Die Struktur orientiert sich stark an der ISO 27001 Norm (Österreichisches Informationssicherheitshandbuch, 2020b).

3.9 Risikoanalysen für Social Engineering

Wenn Objekte oder Informationen im Unternehmen besondere Schutzziele wie Vertraulichkeit, Integrität und Verfügbarkeit (Kapitel 2.2) aufweisen, bzw. benötigen, ist eine Risikoanalyse erforderlich (Anleitung zur Migration von Sicherheitskonzepten, 2018).

Für eine Identifizierung von Risiken muss organisationsweit mit allen Abteilungen und Prozessverantwortlichen zusammengearbeitet werden, um die notwendige Grundlage für Maßnahmen zur Risikominimierung zu schaffen (Decker, 2017).

Eine Kennzahl, mit der Unternehmen Kosten und Nutzen von Risikomanagement berechnen können, wird in der IT-Sicherheit als Return On Security Invest (ROSI) bezeichnet. Mit einer Formel wird der Nutzen mit den Kosten eines Risikomanagementsystems in ein Verhältnis gebracht, um zu berechnen, ob sich die Einführung lohnt (Witt, 2006).

$$ROSI = \frac{(RS * RV) - AK}{AK}$$

Formel 1: Return On Security Invest

RS= Risikosumme

RV= Risikoverminderung

AK= Anschaffungskosten

Zur Implementierung eines unternehmenseigenen Risikomanagements stehen viele verschiedene Rahmenwerke zur Verfügung, die eine systematische Analyse und Bewältigung von Risiken zur Informationssicherheit ermöglichen. Sehr oft wird auch ein kombinierter Ansatz von mehreren Rahmenwerken angestrebt (Beißel, 2017; *Österreichisches Informationssicherheitshandbuch*, 2021).

Einen Überblick über die verbreiteten Rahmenwerke für Risikomanagement und welche für die unterschiedlichen Unternehmen und Einsatzszenarien geeignet sind, stellt Beißel (2017) in seiner Publikation vor. Abbildung 3.11 zeigt die untersuchten Rahmenwerke mit ihren Teilschnitten.

Tab. 1 Teilschritte der Rahmenwerke

	COBIT	CRAMM	FAIR	FRAAP	ISO 31000/M_o_R	OCTAVE-S	RMF	TARA
1	Risikoidentifikation	Identifikation und Bewertung von Vermögensobjekten	Identifikation von Szenario-Komponenten	Pre-FRAAP	Kontext schaffen	Erstellung von Bedrohungsprofilen	Kategorisierung eines IT-Systems	Messung von aktuellen Risiken durch Agenten
2	Risikoevaluation	Evaluation von Bedrohungen und Schwachstellen	Evaluierung der Häufigkeit von Schadensereignissen	FRAAP-Session	Risiken identifizieren	Identifikation von Infrastruktur-Schwachstellen	Auswahl von Sicherheitskontrollen	Identifizieren von Agenten mit hohen Risiken
3	Risikobewältigung	Selektion von Gegenmaßnahmen und Empfehlung	Evaluierung der erwarteten Schadenshöhe	Post-FRAAP	Risiken analysieren	Entwicklung von Sicherheits--Strategie und -Plan	Implementierung von Sicherheitskontrollen	Ableiten der Ziele dieser Agenten
4	Überwachung von Risiken und Kontrollen sowie Berichterstattung	–	Ableitung von Risiken	–	Risiken bewerten	–	Bewertung von Sicherheitskontrollen	Identifizieren von Methoden
5	–	–	–	–	Risiken behandeln	–	Autorisierung der IT-Systeme	Feststellung der wichtigsten Bedrohungen
6	–	–	–	–	Überwachung und Bewertung	–	Überwachung der Sicherheitskontrollen	Anpassen der Unternehmensstrategie

Abbildung 3.11: Übersicht/Teilschnitte der Rahmenwerke (Beißel, 2017)

In der nachfolgenden Abbildung (3.12) werden die Besonderheiten der von Beißel (2017) analysierten Rahmenwerke illustriert.

Rahmenwerke	Besonderheiten
COBIT for IT Risk	Teil eines umfassenderen Rahmenwerks (COBIT), Aufbau auf COBIT-Prinzipien
CRAMM	Starre Struktur, Überblick über viele Schutzmaßnahmen
FAIR	Quantitative Risikobewertungen, Glossar für viele Begriffe
FRAAP	Schnelle Ergebnisse, Eingrenzung auf ein einzelnes Vermögensobjekt
ISO 31000/M_o_R	Idealtypischer Ablauf, hohe Berücksichtigung von Kontext und Zielen
OCTAVE-S/ OCTAVE Allegro	Hohe Verbreitung, Gruppierungsansätze
RMF	Fokussierung auf IT-Systeme
TARA	Analyse von Personen und Gruppen
RMM	Beurteilung des IT-Risikomanagements

Abbildung 3.12: Besonderheiten der Rahmenwerke (Beißel, 2017)

Die diskutierten Rahmenwerke für das IT-Risikomanagement unterscheiden sich in ihrem Inhalt, ähneln sich jedoch in den Phasen, die grundsätzlich in jedem Framework enthalten sind: Identifikation von Risiken, Analyse von Risiken und Bewältigung von Risiken. In den Schwerpunkten sind jedoch Unterschiede erkennbar (Beißel, 2017).

Bei der Risikoidentifizierung werden für gewöhnlich zwei Ansätze herangezogen.

- Ereignis-basierender Ansatz: Hier werden mögliche Ereignisse und ihre Folgen identifiziert, die auf historische, oder theoretische Daten bzw. Expertengutachten gestützt sind. Diese Vorgehensweise kann ohne große Mühen unternommen werden. Aufgrund der nicht systematischen Vorgangsweise können Bedrohungen leicht übersehen werden.

- Auf Werten, Bedrohungen und Schwachstellen basierender Ansatz: Der ursachenorientierte Ansatz, bei dem durch die detaillierte Betrachtung von Werten, Bedrohungen und Schwachstellen mögliche Risiken explizit abgeleitet werden, erlaubt eine systematische und zielgerichtete Vorgangsweise zur Identifizierung der Risiken. Der Nachteil bei diesem Ansatz ist der große Aufwand.

Die Schwachstellen können nach der Risikomanagement Norm ISO/IEC 27005:2011 klassifiziert werden. Personal oder Mitarbeiterinnen und Mitarbeiter können als Gefahr für die Informationssicherheit identifiziert und in einen Schwachstellenkatalog klassifiziert werden (Decker, 2017).

Die Berücksichtigung der Gefahren von Social Engineering liegt bei der Implementierung von Risikomanagementsystemen im Ermessen des Erstellers. Besonders Risiken, die durch Fehlverhalten des Menschen eintreten können, müssen gesondert betrachtet werden. Ein Ansatz zur Untersuchung und Beurteilung menschlichen Fehlverhaltens findet sich in der Risikomanagementmethode Human Reliability Analysis (HRA) (Klipper, 2020).

HRA konzentriert sich auf eine Einschätzung möglichen Fehlverhaltens von Arbeitskräften. Bei der Analyse werden folgende Aspekte untersucht und ausgewertet:

- Was kann falsch sein?
- Was sind die Folgen?
- Welche Faktoren beeinflussen die Zuverlässigkeit?
- Was ist notwendig, um die Zuverlässigkeit zu verbessern und Risiken zu minimieren?

Für die Auswahl der geeigneten Methoden zur Beantwortung der Fragen ist es notwendig, die Grundkonzepte der menschlichen Zuverlässigkeit zu verstehen.

Folgende Fehler können bei der Analyse berücksichtigt werden:

- Unterlassungsfehler, aufgrund eines Versehens oder einer Fehlwahrnehmung.
- Ausführungsfehler bei der Durchführung einer Tätigkeit.

- Vorsätzliche Fehler, wenn bewusst schädliche Handlungen ausgeführt werden.

Die Methodenauswahl soll je nach Zielsetzung erfolgen. Dabei ist es ratsam, verschiedene Methoden aus dem Rahmenprogramm von HRA miteinander zu kombinieren, um die menschliche Fehlerwahrscheinlichkeitsrate positiv beeinflussen zu können (Calixto, 2016).

3.10 Ableitungen aus den aktuellen Forschungsergebnissen

Unternehmen müssen bei der Einsetzung von Sicherheitsrichtlinien die eigenen Mitarbeiterinnen und Mitarbeiter als Fehlerquelle einkalkulieren. Wie viele Studien bereits zeigten, öffneten viele Arbeitnehmerinnen und Arbeitnehmer selbst unmittelbar nach der Sicherheitsunterweisung diverse mit Schadsoftware verseuchte Dateien (Klipper, 2020).

Bequemlichkeit spielt ebenso eine große Rolle. Oftmals wurde vom Autor dieser Publikation beobachtet, dass durch technische Maßnahmen gesperrte E-Mail Anhänge oder mit Makros behaftete Dateien durch unzulässige Hilfsmittel oder Manipulation von Geräten umgangen wurden, um ungeprüfte Dateien in das Firmennetzwerk hochzuladen, nur um aufwändigen Prüfungs- und Genehmigungsverfahren ausweichen zu können. Der Social Engineer nutzt diese Schwächen geschickt aus.

Design Paradigmen wie Security By Design oder Fail Safe, werden so konzipiert, dass bereits vor der Erstellung des Pflichtenheftes und der Verwirklichung von IT-Systemen und Prozessen von Beginn an technische und menschliche Fehler berücksichtigt werden.

CISO werden bei der Erstellung nicht immer eingebunden und haben oft wenig Einfluss auf das notwendige Budget und Handlungsfreiheit für Sicherheitsmaßnahmen in den Abteilungen (*Welche Aufgaben ein CISO übernehmen muss*, 2021).

Das Hauptaugenmerk der Unternehmen und Sicherheitsverantwortlichen liegt meistens auf technologischer Abstützung von Sicherheitsmaßnahmen und weniger auf einer ganzheitlichen Sicherheitsstruktur und -kultur, die von allen Bediensteten akzeptiert und auch gelebt wird.

Besonders für KMU ist die Umsetzung eines Compliance Management-Systems aufgrund der eingeschränkten Kapazität schwierig. (Deistler & Rentrop, 2020).

Wie bereits in der Einleitung dargelegt, ist es zwingend notwendig, dass CISO bei allen Prozessen im Unternehmen aktiv eingebunden werden, um den Faktor Sicherheit in alle Prozesse zu implementieren und überwachen zu können.

4 Vorgehensweise und Methoden

Um einen Erkenntnisgewinn zur Beantwortung der Forschungsfragen und Generierung einer Handlungsempfehlung erreichen zu können, bedarf es der Anwendung wissenschaftlicher Methoden. Die unterschiedlichen Praktiken und Paradigmen der Wissenschaft erfordern besondere Methodenkompetenz und Planung der inhaltlichen-, methodischen-, forschungsökonomischen- und ethischen- Aspekte der empirischen Forschung.

Eine exakte Zuordnung dieser Publikation zu einem bestimmten Forschungsbereich ist nicht eindeutig möglich, da sowohl Forschungsparadigmen der Wirtschaftsinformatik als auch der Sozial- und Humanwissenschaften bei der Analyse des Untersuchungsgegenstandes auftreten.

Während der Themenbereich der Informationssicherheit eindeutig den Ingenieurwissenschaften als zentralem Untersuchungsgegenstand zuzuordnen ist, kann man den Faktor Mensch eher den Humanwissenschaften zurechnen (Döring & Bortz, 2016a, S. 12, 23).

Die Wirtschaftsinformatik vereint behavioristische und konstruktionsorientierte Forschung und entwickelt Modelle für Informations- und Kommunikationssysteme, um diese Systeme zu untersuchen und ihr spezifisches Verhalten erklären zu können. Dazu zählen auch Prognosen für Wirtschaft- als auch der sozialwissenschaftlichen Betrachtungsweise zur Aufgabenerfüllung.

Die Wirtschaftsinformatik beschäftig sich mit der Struktur von Mensch/Aufgabe/Technik-Systemen (MAT-Systemen), die in der Wirklichkeit existieren und beobachtet werden können. Diese gilt es ziel- und zweckorientiert zu nutzen und zu gestalten (Heinrich et al., 2011, S. 3).

Heinrich et al. (2011) charakterisieren die in der Wirtschaftsinformatik spezifischen Forschungsmethoden für empirische Studien als Problemlösungsverfahren und zählen folgende Methoden auf:

- Aktionsforschung
- Befragung
- Ethnographie
- Fallstudie
- Feldexperiment
- Hermeneutik
- Inhaltsanalyse
- Laborexperiment
- Simulation
- Synopse

Grundsätzlich unterscheidet man in der empirischen Forschung zwei Forschungsansätze, deren Grundzüge unterschiedlich sind. Überprüfende versus entdeckende Forschungslogik. Hinzu kommt die Unterscheidung zwischen dem quantitativen (überprüfende) sowie dem qualitativen (entdeckende) Forschungsprozess (Döring & Bortz, 2016a, S. 12).

Im Rahmen von quantitativen Forschungsmethoden werden bestehende Theorien bereitgestellt, um daraus Hypothesen abzuleiten und diese mithilfe von Variablen zu überprüfen. Diese Vorgangsweise erfordert signifikant höhere Messgrößen als im entdeckenden Ansatz, um die zuvor generierten Hypothesen entweder widerlegen oder bestätigen zu können (Brüsemeister, 2008, S. 20).

Das Ziel des qualitativen Forschungsansatzes hingegen ist die Entdeckung von neuen Theorien durch empirische Methoden. Im Rahmen dieser Publikation wurde der qualitative Forschungsansatz ausgewählt, um die Forschungsfrage zu beantworten. In diesem Kapitel wird die Auswahl des Forschungsansatzes sowie die Datenerhebung detailliert beschrieben und begründet.

4.1 Begründung des Forschungsdesigns

Da keine Datensätze vorhanden sind, müssen diese durch eine Primärstudie bzw. Primäranalyse selbst erhoben werden (Döring & Bortz, 2016a, S. 191).

Für den bislang wenig untersuchten Gegenstand wird ein explorativer Forschungsansatz ausgewählt, um das Problem zu erkunden und neue Theorien zu entwickeln. Dazu wird ein qualitativer Forschungsprozess angewendet. Auf Grundlage der offenen Forschungsfrage, werden durch ein nicht-standardisiertes Erhebungsinstrument in Form einer explorativen Interviewstudie mit ExpertInnen die Datensätze erhoben und diese anhand der qualitativen strukturierten Inhaltsanalyse nach Mayring zu theoretischen Konzepten ausgeprägt und verdichtet.

Die ExpertenInnen werden abschließend über mögliche Handlungsempfehlungen befragt, welche anschließend mittels argumentativer Schlussfolgerungen abgerundet werden. Dabei wird induktiv vorgegangen und durch Abstraktion übergeordneter theoretischer Begriffe werden die Konzepte gebildet (Döring & Bortz, 2016a, S. 222).

4.2 Qualitativer Forschungsprozess- Operationalisierung

Wie in der Einleitung zu diesem Kapitel bereits erwähnt, wird in der empirischen Forschung zwischen dem qualitativen und dem quantitativen Forschungsansatz unterschieden, die unterschiedliche Vorgehensweisen erfordern. Während der quantitative Forschungsprozess sich eines sequentiell strukturierten Prozesses quantitativer bzw. numerischer Daten bedient, welche mit statistischen Methoden analysiert werden, verwendet der qualitative Forschungsprozess iterativ amorphe Praktiken der Datenerhebung.

Dabei kommen nicht- numerische Daten zum Einsatz, wie etwa aus Text, Bild oder aus der Beobachtung gewonnener Informationen und werden anschließend interpretativen Analysen unterzogen und ausgewertet. Der „Mixed Methods-Ansatz“ vereint beide Paradigmen in einer Studie.

Ziel des qualitativen Forschungsansatzes ist das Generieren von neuen Theorien und Hypothesen. Dabei wird von einer Operationalisierung einzelner Variablen Abstand genommen.

Die aus kleinen Stichproben anhand von Einzelfällen gesammelten Daten werden zirkulär analysiert und dadurch schrittweise die weiteren Datenerhebungen strukturiert, um die Rohdaten in der abschließenden Phase zu neuen Theorien bzw. Hypothesen zu verdichten. Die nachfolgende Abbildung (4.1) veranschaulicht den zirkulären qualitativen Forschungsprozess (Döring & Bortz, 2016a, S. 26–27).

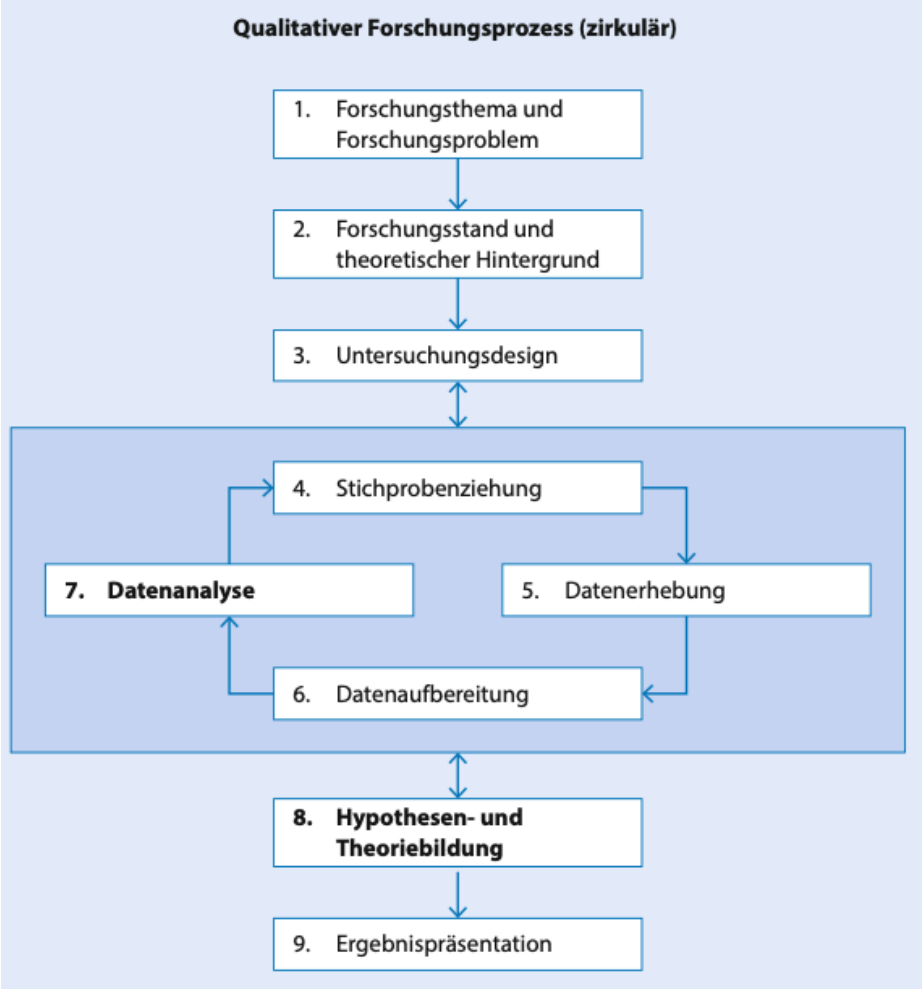

Abbildung 4.1: Qualitativer Forschungsprozess (Döring & Bortz, 2016a, S. 27)

Vor allem in der qualitativen Forschung hat sich die Induktion[10] etabliert, bei der aus den Einzelfällen Muster identifiziert und neue Theorien gebildet werden können. Die induktive Bildung der theoretischen Konzepte erfolgt in drei Ebenen, wie von Döring& Bortz (2016) beschrieben.

1. Empirische Ebene: Datenerhebung
2. Operationalisierung: Interpretation und Verdichtung der Daten
3. Theoretische Ebene: Bildung von Theorien als Ergebnis der qualitativen Studie.

4.3 Erhebung der Daten

Die Datenerhebung ist ein zentrales Element jeder Studie. Sie stützt sich auf verschiedene Methoden, die sich voneinander in der jeweiligen Vorgehensweise, dem Aufwand und dem Informationsgehalt unterscheiden und genau für den Einsatz evaluiert werden müssen.

Im Vergleich zu den von Heinrich et al. (2011) erläuterten Forschungsmethoden der Wirtschaftsinformatik (Einleitung Kapitel 4) klassifizieren Döring & Bortz (2016) sechs divergente Datenerhebungstechniken, welche mit Ausnahme der psychologischen Messung als qualitative Forschungsmethoden herangezogen werden (Döring & Bortz, 2016b, S. 376).

- Beobachtung
- Interview (mündlich)
- Schriftliche Befragung bzw. selbstadministrierte Fragebogenmethode
- Psychologischer Test
- Psychologische Messung
- Dokumentenanalyse

[10] Schlussfolgerung vom Speziellen auf das Allgemeine

Die nachfolgende Tabelle 1 zeigt die in Anlehnung an Döring & Bortz (2016) untersuchten Varianten des qualitativen Interviews und deren Einordnung.

Hier wird zuerst nach dem Grad der Strukturierung unterteilt und anschließend kategorisiert. Aufgrund dieser Zuordnung erfolgte die Auswahl der in dieser Publikation verwendeten Datenerhebungstechnik.

Unstrukturiertes Interview	Halbstrukturiertes Interview
Einzelinterview/ Gruppen-interview Narratives Interview Methode des lauten Denkens Ethnografisches Feldinterview	Leitfadengestütztes Interview Tel/Online Leitfadengestütztes Interview Experten-Interview Problemzentriertes Interview

Tabelle 1: Varianten des qualitativen Interviews (Döring & Bortz, 2016a)

4.3.1 Leitfadengestütztes Experteninterview

Aufgrund der Forschungsfrage und der abzuleitenden Handlungs-empfehlungen ist es notwendig, bei der Datenerhebung auf fachspezifisches Wissen von ExpertInnen Bezug zu nehmen. Die Befragten werden aufgrund deren Erfahrung, Ausbildung und spezifischem Rollenwissen ausgewählt.

Ein Stichprobenplan unterstützt bei der Auswahl der ExpertInnen, die oft schwerer zu erreichen und in geringerer Anzahl verfügbar sind als bei anderen Interviewmethoden (Döring & Bortz, 2016a, S. 375).

Eine weitverbreitete Methode qualitative Daten zu erheben, sind leitfadengestützte Interviews.

Durch den vorab erstellten und systematisch eingesetzten Leitfaden wird die Steuerung des Interviews mit ExpertInnen ermöglicht. Sie beruht auf dem Prinzip „So offen wie möglich, so strukturiert wie notwendig“. Auch wenn man dem Grundsatz der Offenheit im qualitativen Ansatz folgen sollte, ist Steuerung des Interviews oft zwingend erforderlich. Der Einsatz von unterschiedlichen Stimuli (Anreize), wie etwa Bilder oder Prozesse, ist im leitfadengestützten Interview möglich (Helfferich, 2019).

Helfferich (2019) beschreibt eine in drei Schritten gegliederte Vorgehensweise für den Aufbau des leitfadengestützten Interviews, um dem Prinzip "offen aber so strukturiert wie möglich" folgen zu können. Den Befragten soll ermöglicht werden, sich offen über den Sachverhalt und die für die Forschung bedeutsamen Blickpunkte ausdrücken zu können.

Bei diesem Schritt werden nur jene Aspekte explizit untersucht, die im ersten Schritt nicht bzw. nicht ausreichend dokumentiert wurden. Dieser Schritt kann daher auch iterativ durchgeführt werden. Im letzten Schritt werden abschließend die strukturierten, vorformulierten Fragen gestellt.

Die nachfolgende Tabelle zeigt ein mögliches Grundmuster eines Leitfadens.

Leitfrage/Stimulus/ Erzählaufforderung	Inhaltliche Aspekte	(Nach)Fragen mit Formulierung
Erzählaufforderung		
Erzählaufforderung		
Bilanzierungsfragen		
Einstellungsfragen		
Abschlussfrage		
Nach dem Interview: Zusätzlicher Fragebogen für Fakten-fragen		

Tabelle 2: Grundmuster für ein leitfadengestütztes Interview (Helfferich, 2019, S. 678)

Ein problemzentriertes Interview ermöglicht eine ausgewogene Balance der Strukturierung und eine induktiv-deduktive Korrelation. Das Hauptaugenmerk liegt auf der gemeinsamen Ausarbeitung eines Problems (Döring & Bortz, 2016a, S. 377; Witzel, 2000). Ähnlich wie beim problemzentrierten Interview liegt der Schwerpunkt beim von Helfferich (2019) beschriebenen Dilemma Interview bei der Gestaltung von Lösungen oder Handlungsempfehlungen. Der Einsatz von Stimuli wirkt sich bei dieser Methode besonders stark auf die Datenerhebung aus. Der Ablauf des leitfadengestützten Interviews dient im Allgemeinen der subjektiven Erhebung der Daten. Dabei kann es notwendig sein, den Befragten, falls erforderlich, wieder zur wesentlichen Thematik zurückzuführen (Helfferich, 2019, S. 679).

Nach Evaluierung der unterschiedlichen Aspekte des Interviews (Tabelle 1) und Auswertung der in der angeführten Literatur beschriebenen Vorgangsweisen zur Erhebung von Daten, wurde die Durchführung eines problemzentrierten, leitfadengestützten Interviews mit ExpertInnen ausgewählt.

4.3.2 Auswahl der Experten

Um Fachleute für das ExpertInneninterview definieren zu können, wurden folgende Kriterien für die Auswahl der InterviewpartnerInnen festgelegt:

- Mindestens fünf Jahre Erfahrung in der IT- und Informationssicherheitsbranche.
- Einschlägige Praxis bei der Planung von Awarenessmaßnahmen und im Betrieb eines Information Security Management Systems (ISMS).
- Umfangreiche Kenntnisse über aktuelle Standards der Informationssicherheit sowie der relevanten Gesetzgebung.

4.3.3 Vorbereitung der leitfadengestützten ExpertInneninterviews

Aufgrund der während der Konzeption dieser Publikation bestehenden Covid-19 Pandemie und daraus resultierenden Schutzmaßnahmen sowie der starken Einschränkung der Bewegungsfreiheit wurden die Interviews mit einem Videokonferenzsystem abgewickelt und der Ton aufgezeichnet.

Die Rekrutierung zur Teilnahme am Interview erfolgte telefonisch und alle Interviewpartner wurden im Vorfeld über die Thematik unterrichtet sowie auf die Audio-Aufnahme des Interviews hingewiesen. Auf eine Videoaufzeichnung wurde vom Autor aus Datenschutzgründen verzichtet, da Video und Bildaufnahmen bei Verlust oder Diebstahl missbräuchlich verwendet werden können. Eine Einwilligungserklärung wurde an alle TeilnehmerInnen im Vorfeld elektronisch versendet, um die notwendigen Unterschriften einholen zu können.

Zusätzlich wurde eine Vertraulichkeitsvereinbarung vorbereitet, falls ExpertInnen eine Erkennbarkeit ihrer Person oder ihres Unternehmens in dieser Publikation vermeiden möchten.

Ein Pre-Test des Interviews wurde im März 2021 mit einem IT-Sicherheitsexperten des Bundesministeriums für Inneres (BMI) durchgeführt. Dadurch konnten kleine Anpassungen an den Leitfragen und der Vertraulichkeitsvereinbarung erfolgen, um mögliche Fehlerquellen weiter zu minimieren. Besondere Erkenntnisse daraus waren etwa die flexible Gestaltung der Fragen und die Durchführung einer Einleitung in die Thematik durch aktuelle Statistiken und Meldungen über Social Engineering Angriffe und Schadenssummen von Cyberangriffen auf Unternehmen in Österreich und Deutschland im Jahr 2020.

4.3.4 Durchführung der leitfadengestützten ExpertInneninterviews

Für das problemzentrierte, leitfadengestützte Interview werden die von Witzel (2000) erläuterten sieben Phasen übernommen und für das Experteninterview umgesetzt (Witzel, 2000).

1. Dem Interviewpartner die Ziele und den Ablauf des Interviews erklären.
2. Erhebung von sozio- und biografischen Informationen, insbesondere über Ausbildung und Beruf.
3. Einleitung als Erzählimpuls. In dieser Phase werden dem Interviewpartner aktuelle Statistiken zu Social Engineering Angriffen vorgelegt.
4. Erzählungs- und verständnisgenerierende Sondierung der Eingangserzählung.
5. Flexible und angepasste ad-hoc-Fragen insbesondere über Handlungsempfehlungen mit Bezug auf Einbindung des Informationssicherheitsbeauftragten in die Modellierung von Geschäftsprozessen und Verbesserungsvorschläge für Sicherheitsschulungen.
6. Unmittelbar nach dem Interview werden Interviewnotizen zusammengestellt.
7. Transkription und Auswertung der Daten.

Der Leitfaden des Interviews wurde in mehrere Themenbereiche unterteilt und nach jedem Interview iterativ adaptiert, um das gewonnene Wissen verdichten zu können und dabei neues Wissen zu generieren. Die aus dem Kapitel 3.10 abgeleiteten Ergebnisse bildeten eine Basis für die Fragestellung.

Folgende Themenbereiche wurden im Interviewleitfaden behandelt:

- Aktuelle Position und Tätigkeiten im Unternehmen/Organisation sowie vorherige arbeitgebende Unternehmen.
- Welche Fähigkeiten ein CISO vorweisen muss und wie diese Funktion in das Unternehmen/Organisation eingebunden werden sollte.
- Social Engineering Angriffe auf das Unternehmen/Organisation.

- Verhalten der Unternehmensleitung in Bezug auf Sicherheit und Einbindung des CISO in die aktive Gestaltung von Geschäftsprozessen.
- Eigene Einschätzung, warum Social Engineering so erfolgreich ist.
- Aktuelles Schulungsangebot im eigenen Unternehmen.
- Handlungsempfehlungen in Bezug auf organisatorische Schutzmaßnahmen und unmittelbar in Verbindung stehende technische Schutzmaßnahmen.

4.3.5 Beschreibung der ExpertInnen

Aufgrund der teils sehr sensiblen Informationen über Sicherheitslücken als auch falsche Einbindung des/der Sicherheitsverantwortlichen in die Unternehmensstruktur sowie Konflikte mit der Geschäftsführung wurden alle InterviewteilnehmerInnen anonymisiert. Informationen, die Rückschlüsse auf das Unternehmen schließen lassen, wurden entfernt oder anonymisiert.

Alle Gesprächspartnerinnen und Gesprächspartner wurden infolge ihrer langjährigen Erfahrung in der IT-Branche ausgewählt.

Obendrein konnten mehrere Sicherheitsverantwortliche bzw. CISO und Information Security Officer (ISO) sowie beratende Fachpersonen für KMU´s hinsichtlich Information Security als ExpertInnen für die Interviews gewonnen werden.

Die nachfolgende Tabelle 3 zeigt eine Auflistung aller acht Interviews mit der Funktion, Branche und Unternehmensgröße, welche durch die Anzahl der Mitarbeitenden abgeleitet werden kann.

Interview Nr.	Funktion im Unternehmen	Branche	Anzahl Mitarbeiter
Interview 1	CISO	Möbelbranche	~8000 MitarbeiterInnen
Interview 2	CISO	Öffentliches Unternehmen	~3000 MitarbeiterInnen
Interview 3	CISO & IT-Leiter	Wirtschafts-prüfung	~1500 MitarbeiterInnen
Interview 4	ISO	Öffentliches Unternehmen	~1500 MitarbeiterInnen
Interview 5	IT-Leiter & Sicherheitsverant-wortlicher	Logistik-branche	~4500 MitarbeiterInnen
Interview 6	Hochschulprofessor	Fachhoch-schule	~700 MitarbeiterInnen
Interview 7	Consultant & Sicherheitsverant-wortlicher	Consulting-Unternehmen IT-Bereich	~50 MitarbeiterInnen
Interview 8	Consultant	Consulting-Unternehmen IT-Bereich	~20 MitarbeiterInnen

Tabelle 3: GesprächspartnerInnen der ExpertenInneninterviews

4.4 Datenaufbereitung

Um sowohl die qualitativen als auch quantitativen Daten systematisch analysieren und die Aussagekraft der verwendeten Daten steigern zu können, müssen die erhobenen, unbehandelten Rohdaten aufbereitet werden. Die aufbereiteten Daten werden allesamt als Datensätze bezeichnet.

Die gründliche Datenaufbereitung minimiert das Risiko, falsche oder fehlerbehaftete Ergebnisse zu interpretieren und ermöglicht zudem eine unkomplizierte Re-Analyse sowohl durch den Forscher selbst als auch für andere ForscherInnen im Zuge einer Sekundäranalyse.

Zusätzlich können ethische Probleme, wie etwa schlecht durchgeführte Anonymisierung von Interviewpartnerinnen und Interviewpartnern und darauffolgende Identifizierung der Experten, durch eine strukturierte Datenaufbereitung vermieden werden (Döring & Bortz, 2016a, S. 580).

Für eine sorgfältige Aufbereitung der Daten werden die von Döring & Bortz (2016) beschriebenen Schritte der Datenaufbereitung angewendet.

- Erstellung
- Kommentierung
- Anonymisierung
- Bereinigung
- Transformation

Die einzelnen Schritte werden in Kapitel 4.5 bei der Durchführung der Datenaufbereitung detailliert beschrieben.

4.5 Datenanalyse - Qualitative Inhaltsanalyse nach Mayring

Experteninterviews lassen sich durch verschiedene Vorgangsweisen auswerten. In der Leitliteratur, insbesondere in Lehrbüchern zu Forschungsmethoden, werden viele Verfahren beschrieben. Diese unterschiedlichen Verfahren lassen sich allesamt unter dem Begriff „qualitative Inhaltsanalyse“ subsumieren.

In vielen deutschsprachigen Lehrbüchern zu dieser Thematik wird auf die qualitative Inhaltsanalyse von Philipp Mayring verwiesen (Döring & Bortz, 2016a, S. 542; Kaiser, 2014, S. 91).

Das allgemeine Ablaufmodell nach Mayring (2015) bietet ein Gerüst zur Unterstützung der quantitativen Analyseschritte. Dabei steht im Mittelpunkt immer die Definition von Kategorien, die iterativ zwischen der konkreten Fragestellung und dem erhobenen Material erstellt und kontinuierlich nachgeprüft werden (Mayring, 2015, S. 61).

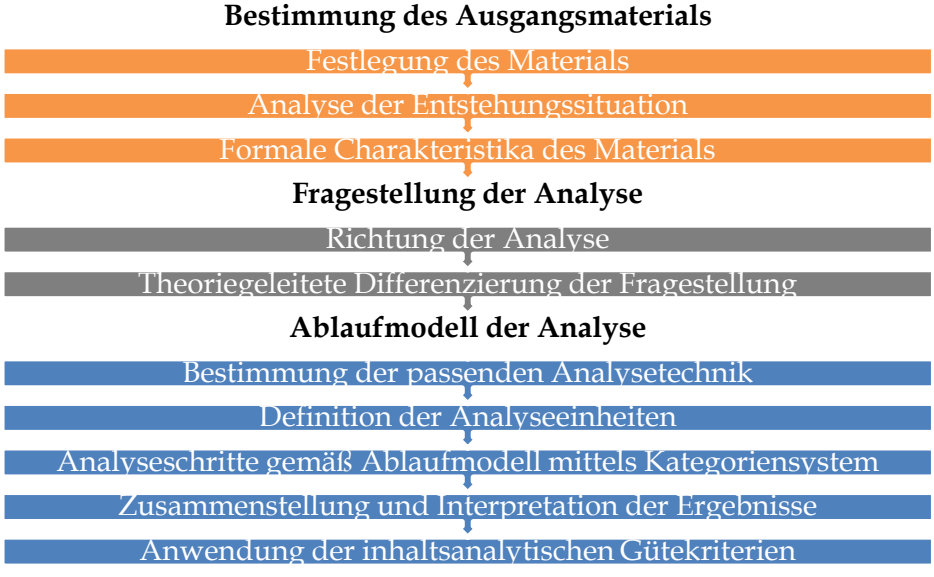

Abbildung 4.2: Allgemeines inhaltsanalytisches Ablaufmodell (in Anlehnung an Mayring (2015)

Die nachfolgenden Schritte beschreiben die Umsetzung des in Abbildung 4.2 dargestellten Ablaufmodelles in der vorliegenden inhaltsanalytischen Auswertung.

4.5.1 Bestimmung des Ausgangsmaterials

Festlegung des Materials:

Das erhobene Datenmaterial für die Auswertung wurde aus den acht ExpertInneninterviews generiert. Die für die Interviews gewonnenen Fachleute wurden aufgrund deren spezifischen Kompetenzen (Kapitel 4.3.2) ausgewählt.

Durch die ständige Anpassung der Fragen im Zuge der Interviews, konnte nach Analyse der Stichprobenziehung kein neues Wissen generiert werden. Somit kann abgeleitet werden, dass das erhobene Material als theoretisch gesättigt gilt.

Analyse der Entstehungssituation:

Die Interviewpartner wurden durch die beruflichen Kontakte des Autors ausgewählt und via E-Mail bzw. telefonisch kontaktiert. Die E-Mail enthielt grundlegende Informationen zur Zielsetzung der Publikation und der Thematik bzw. Problematik von Social Engineering.

Die leitfadengestützten Interviews fanden freiwillig statt und wurden wegen der zur Zeit der Erstellung dieser Publikation anhaltenden Covid-19 Pandemie mittels Videotelefonie (Microsoft Teams sowie Zoom) umgesetzt, wobei nur Tonaufnahmen gespeichert wurden. Zusätzlich stimmten alle Interviewpartner der Einverständniserklärung (mündlich oder schriftlich) zu, die im Vorfeld versendet wurde.

Formale Charakteristika des Materials:

Die im Audioformat m4a gespeicherten Audioaufnahmen der Interviews wurden vollständig unter Einsatz der Software MAXQDA digital transkribiert und zur Überprüfung der Gütekriterien den Gutachtern dieser Publikation zu Verfügung gestellt. Die Audioaufnahmen wurden nach Abgabe der Publikation vernichtet, um eine Identifizierung der Interviewpartner ausschließen zu können.

Nachfolgende Transkriptionsregeln wurden angewendet:

- Die Begrüßung, Zustimmung sowie Verabschiedung wurden nicht transkribiert.
- Die Namen der Experten sowie der Unternehmen/Organisationen wurden mit den jeweiligen Initialen legendiert, um Rückschlüsse auf Personen und Unternehmen/Organisationen ausschließen zu können.
- Die Transkripte wurden bei groben Fehlern grammatikalisch richtiggestellt.
- Dialekte wurden in Hochsprache transkribiert.
- Die Unterscheidung der am Interview beteiligten Personen wurde abgekürzt und in der Legende des jeweiligen Transkripts beschrieben.
  (Experte = E, Interviewer = I).
- Längere Unterbrechungen wurden durch drei Punkte in Klammern (...) dargestellt.
- Das Gesamtmaterial der Transkription befindet sich im Anhang dieser Publikation.

4.5.2 Fragestellung der Analyse

Richtung der Analyse:

Durch die weitreichende berufliche Erfahrung der Experten entwickelte sich eine Situation, in der die Interviewpartner ihre Erfahrungen im Umgang mit Informationssicherheit beschrieben und Handlungsempfehlungen mit Bezug zum Kontext besprochen wurden.

Theoriegeleitete Differenzierung der Fragestellung:

Die Interviewpartner wurden mit der Problematik von Social Engineering Angriffen und der in der Einleitung beschriebenen strukturellen Situation von CISO und Sicherheitsbeauftragten und des begrenzten Handlungsspielraums für die Mitgestaltung von Prozessen in Unternehmen konfrontiert. Die in den Interviews angewendete Struktur der Leitfäden wurde in Kapitel (Kapitel 4.3.4) erläutert.

Im Anschluss an diesen Schritt folgt die Definition des ausgewählten Ablaufmodells sowie der integrierten Technik zur Zergliederung und Untersuchung (Mayring, 2015, S. 61). Die nächsten Schritte des Ablaufmodells (Abbildung 4.2) werden im nachfolgenden Kapitel erklärt.

4.5.3 Ablaufmodell der Analyse

Bevor die zentrale Technik zur Kategorisierung ausgewählt wird, muss beurteilt werden, welche Ziele mit der Analyse erreicht werden sollen (Mayring, 2015, S. 65).

Um im Kontext der Forschungsfrage und des geplanten Zieles eine Handlungsempfehlung aus den Ergebnissen der Datenerhebung zu generieren, wird die Technik nach der von Mayring (2015) dargestellten drei Hauptkategorien von Texten herangezogen (Mayring, 2015, S. 68).

Mayring (2015) unterscheidet dabei drei analytische Techniken der qualitativen Inhaltsanalyse:

- Zusammenfassung: Das Datenmaterial auf die wesentlichen Inhalte abstrahieren, sodass übersichtliche Aussagen geschaffen werden.
- Explikation: In diesem Schritt wird ergänzendes Material zu den Daten hinzugefügt, um Interpretationen erweitern zu können.
- Strukturierung: Analyse und Zuordnung des Materials in vorher definierte Kategorien und anschließende Einschätzung aufgrund der Kriterien.

Aufgrund der Forschungsfrage und Literaturanalyse, sowie die daraus resultierenden Ableitungen (Kapitel 3.10), wurden die Leitfragen und die Phasen des Interviewleitfadens für die deduktive Gliederung der Kategorien zugrunde gelegt. Dies bildete die Grundlage für die Auswahl der strukturierenden qualitativen Inhaltsanalyse nach Mayring.

Bestimmung der Analysetechnik:

Im nächsten Schritt des in Kapitel 4.5. beschriebenen allgemeinen inhaltsanalytischen Ablaufmodells wird nach der Evaluierung der drei beschriebenen Techniken die Analysetechnik der Strukturierung ausgewählt, um eine Handlungsempfehlung aus der Datenerhebung ableiten zu können.

Die laut Mayring (2015) zentralste inhaltsanalytische Technik filtert vorher definierte Kategorien aus dem Datenmaterial. Diese werden nach unterschiedlichen Betrachtungsweisen der Strukturierung (formal, typisierend und skalierend) unterschieden und eignen sich besonders für die theoriegeleitete Analyse von Daten.

Folgende Bausteine werden für die weitere Vorgehensweise benötigt:

1. Darlegung der Kategorien: Exakte Einteilung, welche Daten in die definierte Kategorie zugeteilt werden.
2. Auswahl von Ankerbeispielen: Daten mit eindeutiger Zuordnung einer bestimmten Kategorie werden als Beispiele dieser Kategorie gruppiert.
3. Festsetzung von Codierregeln: Wenn Textstellen nicht eindeutig einer Kategorie zugeordnet werden können, gewährleisten Codierregeln eine Zuordnung.

Das in Abbildung 4.3 dargestellte Modell zeigt den von Mayring (2015) erstellten Ablauf der Strukturierungstechnik. Die zuvor beschriebenen Bausteine leiten die Auswertung ein. Abschließend werden die ausgewerteten Daten aufbereitet und analysiert.

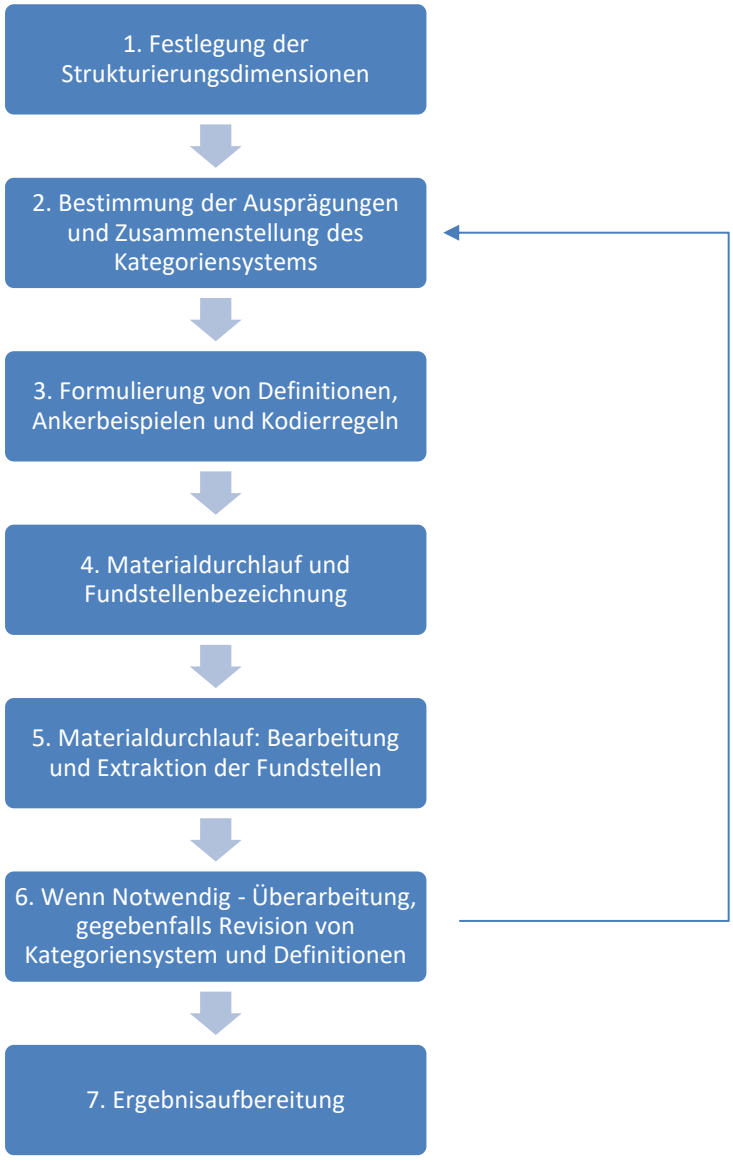

Abbildung 4.3: Ablaufmodell strukturierter Inhaltsanalyse (Mayring, 2015)

Definition der Analyseeinheit:

Im nächsten Schritt werden nach der Bestimmung der Analyseeinheit die Codiereinheiten festgelegt.

Analyseschritte gemäß Ablaufmodell mittels Kategoriensystem:

Die zuvor beschriebenen Analyseschritte gem. Mayring (2015) wurden für die weitere deskriptive Vorgangsweise umgesetzt. Dazu wurde die Software MAXQDA verwendet.

1. Exakte Zuordnung der Textbestandteile in die Kategorien. Die Hauptkategorien wurden dazu aus der Theorie abgeleitet und bildeten die Grundlage des Interviewleitfadens. Die Unterkategorien wurden induktiv aus den erhobenen Daten erstellt.
2. Für die Festlegung von Ankerbeispielen der bestimmten Kategorien wurden eindeutige Textpassagen aus den Interviews verwendet.
3. Codierregeln definieren, um eine eindeutige Zuordnung zu den Kategorien ermöglichen zu können.

Die nachfolgende Tabelle 4 zeigt ein Beispiel der Durchführung.

Codes	Definitionen	Ankerbeispiele	Codierregeln
Handlungs-empfehlungen	Allgemeine Handlungs-empfehlungen von Social Engineering Awareness-Maßnahmen	(...) Rollenspiele für das bessere Verständnis wären eine optimale Lösung von Sicherheitsschulungen (...)	Nur Aussagen im Zusammenhang mit der Fragestellung nach Handlungs-empfehlungen oder Schulungsmaßnahmen

Tabelle 4: Beispiel der Analyseschritte und Definition der Codierregeln

Zusammenstellung und Interpretation der Ergebnisse:

Zum Abschluss werden die ausgewerteten Daten zusammengestellt und interpretiert. Diese Ergebnisse müssen den inhaltsanalytischen Gütekriterien entsprechen, die im nächsten Schritt beschrieben werden. (Kapitel 5)

Anwendung der inhaltsanalytischen Gütekriterien:

Nachfolgend angeführte Gütekriterien der qualitativen Inhaltsanalysen müssen bei der Erhebung und Auswertung der Daten berücksichtigt werden (Göhner & Krell, 2020).

- Validität und Gültigkeit
- Reliabilität
- Transparenz
- Objektivität
- Nähe zum Gegenstand
- Interpretativität
- Praktische Relevanz
- Ethische Überlegungen
- Kommunikativität
- Offenheit

5 Ergebnisse

Nach Erhebung und Analyse der Daten erfolgte die in Kapitel 4.5.3 beschriebene strukturierte Inhaltsanalyse nach Mayring. Die Ergebnisse der insgesamt acht ExpertInneninterviews werden in diesem Kapitel dargestellt und diskutiert. Zitate der ExpertInneninterviews werden exemplarisch je nach Unterkategorie wiedergegeben.

Die Kategorienauswahl erfolgte aufgrund der aus der Literatur abgeleiteten Problematik von Social Engineering (Kapitel 3.10) und begründete die Auswahl der deduktiven Kategorienbildung. Die nachfolgende Tabelle 5 illustriert die fünf deduktiv abgeleiteten Kategorien und induktiv abgeleiteten Unterkategorien.

1. Social Engineering Angriffe auf das Unternehmen
• Erkannte Angriffsarten
• Aufgetretene Probleme
• Berichtete Schäden
• Umgang mit den Angriffen
2. Warum Social Engineering so erfolgreich ist
• Betrachtungsweise Menschen/Mitarbeitende
• Betrachtungsweise Unternehmensleitung/Geschäftsführung
3. Aktueller Ist-Zustand über Position und Befugnisse des Sicherheitsverantwortlichen

• Position und Aufgabenbereiche/Befugnisse des Sicherheitsverantwortlichen
• Konflikte im eigenen Unternehmen oder mit dem Mutter-/Tochterunternehmen
4. Schulungsangebot im eigenen Unternehmen
• Theorie-Schulung
• Häufigkeit und regelmäßige Aktualisierungen
• Verpflichtende Schulungen und Abschlussquizz
• Praktische Schulungen und Penetrationstests
5. Handlungsempfehlungen der Experten
• Handlungsempfehlungen zur Eingliederung des Sicherheitsverantwortlichen
• Handlungsempfehlungen für Sicherheitsschulungen und Penetrationstests
• Handlungsempfehlungen für die physische Sicherheit
• Handlungsempfehlungen für technische Schutzmaßnahmen
• Handlungsempfehlungen für organisatorische Schutzmaßnahmen

Tabelle 5: Alle Kategorien und Unterkategorien

5.1 Kategorie 1: Social Engineering Angriffe auf das eigene Unternehmen

Diese Kategorie beschreibt Social Engineering Angriffe, welche die ExpertInnen in ihren derzeitigen bzw. auch in anderen Unternehmen erfahren haben. Eine Unterkategorie fasst den Umgang mit diesen Angriffen sowie die aufgetretenen Probleme zusammen. Weiters werden Einschätzungen von Trends betreffend Social Engineering Angriffen diskutiert, die von den ExpertInnen in den Unternehmen aufgefunden wurden. Die Gesamtanzahl aller codierten Elemente in dieser Kategorie beträgt 71, wobei folgende fünf Unterkategorien (Tabelle 6) gebildet und die Elemente zusammengefasst wurden.

Social Engineering Angriffe auf das Unternehmen
• Erkannte Angriffsarten
• Aufgetretene Probleme im Zuge der Angriffe
• Berichtete Schäden
• Umgang mit den Angriffen

Tabelle 6: Kategorie 1 mit Unterkategorien

5.1.1 Erkannte Angriffsarten

Die ExpertInnen berichteten relativ wenig über erkannte bzw. gemeldete Social Engineering Kampagnen. Sechs von acht ExpertInnen meldeten Phishing- und Spear-Phishing Angriffe als einzige Angriffsvektoren, wobei grundsätzlich ein sehr starker Trend exakt gezielter Angriffe wie Whaling zu erkennen ist.

> *„Was wir sehr stark verzeichnen, ist Phishing. Da haben wir in den letzten Jahren meiner Meinung nach einen starken Zuwachs gehabt.*

> *Darüber hinaus (...) vor allem im höheren Management merkt man, dass es immer wieder zu Whaling Angriffen kommt, wo wirklich versucht wird, gezielt mit gefälschten E-Mails jemanden im höheren Management zu Handlungen zu bewegen."* (Interview 4: 19)

Besonders im Finanzbereich wird seitens Krimineller sehr stark mit Social Engineering gearbeitet. Aber auch KMU´s stehen aktuell sehr stark im Fokus der Angreifer.

Nur in zwei der befragten Unternehmen wurde vereinzelt über andere Social Engineering Angriffe wie Tailgaiting oder Telefonanrufe im Unternehmensalltag berichtet. Einer der Interviewpartner berichtete sogar über regelmäßige Ausspähungen der Auslandsmitarbeiter durch fremde Nachrichtendienste.

5.1.2 Aufgetretene Probleme im Zuge der erfolgten Angriffe

Eine der größten Problematiken liegt bei fast allen Unternehmen beim Meldeweg für Sicherheitsvorfälle. Nur in sehr wenigen Unternehmen hat sich eine offene Fehlerkultur entwickelt, bei der Mitarbeitende darüber berichten, Opfer eines Angriffes geworden zu sein.

Die Sicherheitsverantwortlichen befürchten, dass nur Informationen zu ihnen gelangen, wenn auch von den Usern eindeutig ein Schaden zu erkennen ist.

> *„Da muss ich sagen (...) fürchte ich, dass nur sehr wenig wirklich bei mir ankommt. Ich glaube sehr vieles davon wird so im Sinne sein (...) wenn nichts passiert ist, dann ist nichts passiert (...) einfach gar nicht weitergeben. Also das ist wirklich sehr selten und dann oft einfach in einem rein informellen Gespräch, dass man vielleicht doch mal hört, dass etwas war. (...) Also wirklich gezielt wird doch nichts weitergeleitet."* (Interview 4: 28-29)

Auch Konflikte zwischen Mutter- und Tochterorganisationen konnten während der Angriffe festgestellt werden. Dabei leiteten die in den Mutterorganisationen hierarchisch höher gestellten CISO nur selten Informationen weiter. Dies ist sehr oft der Firmenpolitik geschuldet, aber auch den persönlichen Befindlichkeiten der einzelnen Funktionen, welche die Kommunikation und die Weiterleitung von Informationen über Angriffskampagnen stark beeinflussen können.

„Wir bekommen nur das übermittelt, was auch die Mutterorganisation uns sagen möchte. Angriffe, die danach ausgesehen haben, dass Angriffe erfolgreich waren, wurden auf Nachfrage nicht bestätigt. Das ist eher Firmenpolitik (...) wahrscheinlich ist es in vielen Firmen so der Fall. Alle schriftlichen Stellungnahmen diesbezüglich wurden negativ beantwortet von der Konzernmutter. Ob das tatsächlich so war, steht in den Sternen. Ich kann nicht das Gegenteil beweisen, auch wenn hier viele Indizien dafürsprechen würden". (Interview 1: 26-29)

5.1.3 Berichtete Schäden

Über tatsächliche Schäden hat nur ein Interviewpartner berichtet, dessen Unternehmensserver zum Teil von einem durch Spear-Phishing eingeschleustem Computervirus infiziert und Daten verschlüsselt wurden. Das Schadensausmaß verursachte einen Aufwand von mehreren Arbeitstagen. Über finanzielle Auswirkungen konnten keine Angaben gemacht werden.

Von den Unternehmen wurde von den Interviewpartnern kein Schaden genannt, weil entweder keiner entstand oder aus Compliance-Gründen keine Informationen darüber erteilt werden konnten, um einen möglichen Reputationsverlust zu vermeiden. Es wird vermutet, dass Anwender aufgrund der bestehenden Angst vor Konsequenzen potenziell aufgetretene Schäden nicht melden.

„(...) und ich glaub, dass die Anwender das einfach nicht reporten, weil es denen möglicherweise peinlich ist, oder weil sie Angst vor Konsequenzen haben." (Interview 6: 26)

Vor allem die beiden Interviewpartner aus dem Consultingbereich bestätigen die hohen Schadenssummen durch diese besondere Angriffsform, können aber aus Gründen der Vertraulichkeit keine konkreten Schadenssummen ihrer Auftraggeberinnen und Auftraggeber nennen.

Die nachfolgende Abbildung 5.1 (nächste Seite) zeigt eine Übersicht über die berichteten Schäden. Es ist hervorzuheben, dass alle acht Unternehmen bereits durch Social Engineering Methoden angegriffen worden sind.

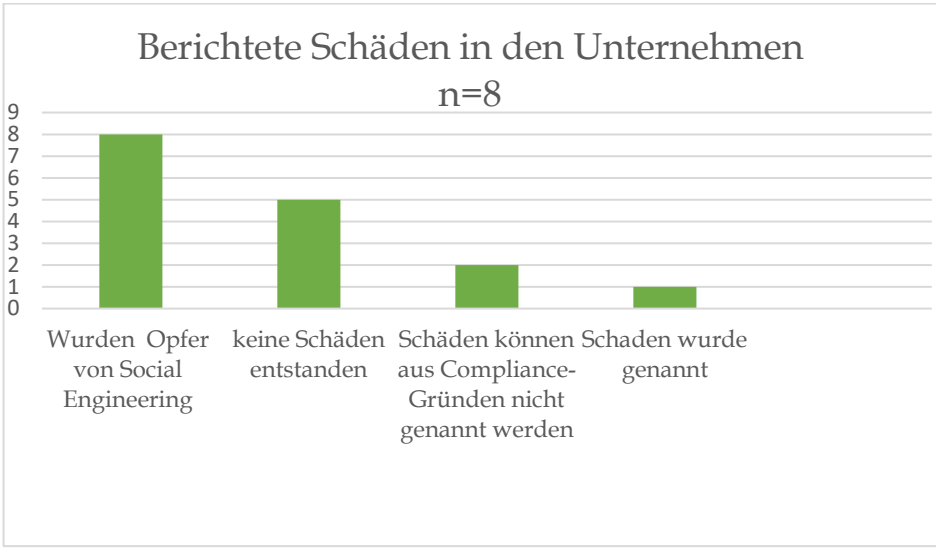

Abbildung 5.1: Berichtete Schäden in den Unternehmen (eigene Abbildung)

5.1.4 Umgang mit den Angriffen

Es wurde unterschiedlich über die Erkenntnisse aufgrund der Angriffe und den resultierenden Schutzmaßnahmen berichtet. Bis auf einen einzigen Sicherheitsverantwortlichen schilderten alle über die Einführung von E-Mail-Zertifikaten, um das Risiko schadhafter E-Mails zu minimieren, welche von Unbekannten oder gefälschten Identitäten versendet werden, und somit die Sicherstellung der Integrität zu gewährleisten.

Die Schwierigkeit bestand darin, diese Zertifikate auch auf den mobilen Geräten zu installieren, da es öfters zu längeren Wartezeiten der Zertifikatsinstallation im Zuge einer Neuanschaffung von Geräten gekommen ist. Durch diese Methode wurden Phishing Angriffe und Spam Nachrichten in den Unternehmen verringert.

Verstärkt wurden auch Security Incident Response Prozesse, bei denen eindeutig festgelegt wird, welche Ansprechperson bei einem Sicherheitsvorfall zu kontaktieren ist. Dabei ist auch eine offene Fehlerkultur wichtig, bei der Mitarbeitende keine Repressalien fürchten müssen, wenn ein Social Engineering Angriff erfolgreich war.

Die Etablierung einer Meldekultur stand hierbei im Vordergrund, um die Sicherheitsverantwortlichen bestmöglich zu unterstützen.

Die technische Umstellung auf Homeoffice hat bei allen Unternehmen grundsätzlich gut funktioniert und wurde nicht als Verstärker für erfolgreiche Angriffe bezeichnet. Es wurde aber allgemein berichtet, dass es sich bei allen Unternehmen um hoch technologisierte Betriebe handelt und sich Homeoffice schon vor der Pandemie in der Firmenkultur erfolgreich etabliert hat.

> *„Die Mitarbeiter dürfen sich dann nicht fürchten, wenn mal was passiert. Da muss man wirklich klar kommunizieren. Er braucht keine Angst haben, weil er jetzt wo drauf geklickt hat.*
>
> *Weil viele Mitarbeiter Angst haben (...) wenn ich das melde, dann reißen sie mir den Kopf ab (...) Nein. Im Gegenteil, wenn man etwas meldet, wird man gelobt, dass man es meldet. Das kann jedem passieren, dass man wo drauf klickt. Das sind wichtige organisatorische Maßnahmen, um auch wirklich in der Organisation alles so zu verteilen und zu kommunizieren (...) Top Down kommunizieren (...) dass da nichts passiert, und dass man da nachschauen kann, wenn man möchte."* (Interview 1: 123-124)

5.2 Kategorie 2: Warum Social Engineering so erfolgreich ist

Warum Social Engineering für Angreifende besonders zielführend ist, wurde im Grundlagenteil (Kapitel 2.5 Psychologische Grundlagen) analysiert. Die interviewten ExpertInnen wurden zu deren persönlichen Einschätzung befragt, warum diese Angriffsart im Allgemeinen für Angreifende so erfolgreich ist.

Diese Hauptkategorie wurde in drei nachfolgende Unterkategorien (Tabelle 7) unterteilt, die aus gesamt 35 Codes bestehen.

Warum Social Engineering so erfolgreich ist
• Betrachtungsweise Menschen/Mitarbeitende
• Betrachtungsweise Unternehmensleitung/Geschäftsführung
• Betrachtungsweise Angreifer/Technologie

Tabelle 7: Kategorie 2 mit Unterkategorien

5.2.1 Betrachtungsweise Menschen/Mitarbeitende

Menschen sind grundsätzlich sehr harmoniebedürftig und versuchen zu helfen. Das gilt natürlich auch für Mitarbeitende. Diese möchten anderen MitarbeiterInnen, KundInnen bzw. LieferantInnen oder anderen Stakeholdern im Bedarfsfall umgehend helfen, um eine Situation für alle Beteiligten positiv ausgehen zu lassen.

Social Engineers suchen sich besonders hilfsbereites und kundenorientiertes Personal als Zielobjekte aus. TrickbetrügerInnen können sehr einfach ihre Ziele erreichen, indem sie ihre potentiellen Opfer in speziellen Situationen unter Ausnutzung ihrer Leichtgläubigkeit und Hilfsbereitschaft entweder telefonisch kontaktieren oder an den Eingangstüren von Firmengeländen direkt ansprechen.

> *„Also aus meiner Sicht ist das ganz einfach und menschlich zu beantworten. Also ich glaub, das liegt in der Natur des Menschen. Jeder Mensch ist harmoniebedürftig, sag ich jetzt mal. Das Individuum Mensch möchte grundsätzlich (...) also ich glaub der Mensch im Durchschnitt (...) möchte helfen (...) möchte gefallen (...) und ist um Harmonie bemüht."* (Interview 3, Pos. 83)

Neugierde und Angst unterstützen die angreifenden Personen bei ihren Tätigkeiten. Menschliche Wesenszüge werden stark ausgenutzt.

Leistungsdruck spielt hier eine verstärkende Rolle. Tätigkeiten müssen immer schneller erledigt werden. Da bleibt oft keine Zeit, um lange darüber nachzudenken, ob sich hinter den vermeintlichen KundInnen ein Angreifender verbergen könnte.

Als zusätzlicher Faktor wurde Unkonzentriertheit in den Interviews genannt. Durch den Leistungsdruck wird auf die schnelle Ausführung der Tätigkeit geachtet. Dabei werden Hinweise über Angriffsversuche übersehen und mögliche Signale ignoriert. Im sehr komplexen Arbeitsalltag mit sehr vielen ineinandergreifenden Geschäftsprozessen wird Unachtsamkeit schnell ausgenützt.

Die Angestellten sind sich nicht bewusst, was technologisch alles möglich ist und wie einfach Social Engineering mit Hilfe von Technologie durchführbar sein kann. Wenn eine E-Mail von anderen Angestellten oder Bekannten kommt, wird dahinter kein Angriff vermutet.

Um diese Angriffe verstehen zu können, wird ebenso privates Interesse gefordert. Das gelte besonders für sehr sensible Rollen, wie etwa die der IT-Abteilung.

> *„Das heißt, selbst die Leute, die in der IT sitzen, (…) wenn die nicht privates, persönliches Interesse an Security haben, gibt es auch genug Administratoren, die dann Blödsinn machen."* (Interview 1: 91)

Der einzige Weg sich vor diesen Angriffen zu schützen, ist Awarenessausbildung.

5.2.2 Betrachtungsweise Unternehmensleitung/Geschäftsführung

Die interviewten ExpertInnen berichteten hier von verschiedenen allgemeinen Problematiken mit deren Funktion sowie der Zusammenarbeit mit der Geschäftsführung. Eine sehr patriarchische Firmenphilosophie spielt gerade bei KMU´s eine große Rolle, weshalb viele Sicherheitslücken nicht beachtet werden. Für Sicherheitsoptimierungen fehlt in solch einer Kultur das Verständnis.

> *„Aber mein Eindruck ist, dass die KMU´s (...) so lange nichts passiert, eher alles ein bisschen salopp und eher locker handhaben, ja."* (Interview 6: 52)

Der Kostenfaktor ist häufig das wichtigste Entscheidungskriterium, das gegen die Implementierung von Sicherheitsmaßnahmen spricht. Die Informationssicherheit wird nicht als Business-Enabler angesehen und Sicherheitsmaßnahmen anderen augenscheinlich lukrativen Projekten nachgereiht.

> *„Die anderen Projekte werden budgettechnisch von der Geschäftsführung immer gegenüber der Sicherheit vorgereiht (...) weil dort der größere Business Value gesehen wird und dementsprechend ist Sicherheit immer zweitrangig"* (Interview 4, Pos. 43).

Die Unternehmerinnen und Unternehmer beurteilen die Sicherheitslage nicht realistisch, da bis dato kein Angriff erfolgte, wodurch sie fälschlicherweise davon ausgehen, dass ihr Unternehmen für AngreiferInnen nicht attraktiv ist. Die ExpertInnen referieren allgemein, dass aufgrund der langen Entscheidungswege nur wenig Sicherheitsinformationen von der Belegschaft an die Sicherheitsfachleute weitergeleitet werden.

5.2.3 Betrachtungsweise Angreifer/Technologie

Angreifende nutzen grundsätzlich immer ausgeklügeltere Methoden und bedienen sich vieler neuer Technologien. Besonders bei der Reproduzierung von Daten und Inhalten werden sie durch den Einsatz von technologischen Hilfsmitteln immer besser.

Bei gut gemachten Angriffen, wie etwa bei der Emotet[11] Angriffswelle, wurden valide E-Mails aus den Exchange Postfächern mit schadhaftem Code verändert und versendet. Die Opfer bemerken bei dieser Malware keine Veränderung, sondern sehen nur den legitimen Absender.

> *„Da sind schon sehr viele gekommen. Ich habe dein Passwort (...) du wurdest da und dort gefilmt (...) dann sind die Mails aber vom Geschäftsführer oder von einer anderen Unternehmensadresse gekommen, weil man den Absender leicht spoofen kann."* (Interview 1: 100).

[11] Emotet ist ein Schadprogramm für Windows – Systeme welches durch echten E-Mail-Verkehr eingeschleust wird.

Der E-Mail-Verkehr bietet hier ein großes Einfallstor für Angreifer. Dabei wird es immer einfacher, einen E-Mail-Verkehr zu spoofen[12]. Die Covid-19 Situation hat den Trend zu Social Engineering Angriffen regelrecht verstärkt. Sehr oft starten diese Angriffskampagnen, die in Wellen auftreten, zeitgleich in verschiedenen Ländern.

Verschiedene neue Geschäftsprozesse, die Nutzung neuer Soft- und Hardware sowie die Nutzung eigener Geräte "Bring Your Own Device" (BYOD), die für den Zugriff auf das Firmennetzwerk genutzt werden, erschwerten zusätzlich die Situation und die Aufgabenbereiche der Sicherheitsverantwortlichen.

Durch diverse Social-Media-Kanäle und Kurznachrichtendienste werden immer mehr Programme und Links zur Kompromittierung von Computersystemen und Netzwerken versendet, die durch die stark zunehmende BYOD Firmenpolitik nicht mehr durch den E-Mail-Exchangefilter entdeckt und blockiert werden können.

> *„Das wird immer schwieriger durch die Bring Your Own Device -Geschichte, Homeoffice, Smartphone. d. h. (...) Im Bereich Phishing bzw. Spear-Phishing ist der Fokus sehr stark gestiegen (…) in meinem Aufgabenbereich."* (Interview 1: 19-20)

5.3 Kategorie 3: Aktueller Ist-Zustand über Position und Befugnisse des Sicherheitsverantwortlichen

Die interviewten ExpertInnen für Informationssicherheit wurden über die derzeitige Situation betreffend der Befugnisse sowie Einbindung der Sicherheitsverantwortlichen in die Unternehmensstruktur befragt. Hier konnten drei Unterkategorien (Tabelle 8) gebildet werden, welche aus gesamt 53 Segmenten bestehen.

[12] Täuschen oder Verschleierung einer Identität

Aktueller Ist-Zustand über Position und Befugnisse des Sicherheitsverantwortlichen
• Position und Aufgabenbereiche/Befugnisse des Sicherheitsverantwortlichen
• Befugnisse des Sicherheitsverantwortlichen
• Konflikte im eigenen Unternehmen oder mit Mutter-/Tochterunternehmen

Tabelle 8: Kategorie 3 mit Unterkategorien

5.3.1 Aktuelle Position und Aufgabenbereiche des Sicherheitsverantwortlichen im Unternehmen

Im Zuge der Befragungen ist besonders aufgefallen, dass viele mit Sicherheitsaufgaben befasste Personen mit einer Doppelfunktion betraut sind. Nur zwei der acht ExpertInnen berichten von einer Funktion als Sicherheitsverantwortlicher ohne jegliche Doppel- oder Zusatzfunktion.

> *„Also ich bin IT- Leiter in meinem Unternehmen, (...) bin aber zusätzlich auch (...) und ob das jetzt gut ist, sei dahingestellt, aber zusätzlich auch für die Security zuständig (...)"* (Interview 3: 7)

Bei der Frage zu den Befugnissen im Unternehmen und die aktive Einbindung bei der Gestaltung von Geschäftsprozessen in Bezug auf Sicherheitsaspekte gaben sieben der acht Interviewpartner an, hier von der Geschäftsführung unterstützt zu werden und zumindest in beratender Funktion bei der Implementierung und Überwachung von Geschäftsprozessen eingebunden zu werden.

5.3.2 Konflikte im eigenen Unternehmen oder mit Mutter-/Tochterunternehmen

Die Doppelfunktion der Sicherheitsverantwortlichen, insbesondere jene mit der IT-Leitung, bringt unterschiedliche Interessenskonflikte mit der Geschäftsführung sowie mit anderen gleichgestellten Abteilungen mit sich. Eine dezidierte Rolle als CISO, welche unmittelbar als Stabsstelle von der Geschäftsführung geführt wird, wäre eine Möglichkeit, diese Konflikte lösen zu können.

> *„Es ist ja eine klassische Unvereinbarkeit. Interessenskonflikt, Leitung IT und ISO. Also auf der einen Seite derjenige der den IT - Betrieb möglichst komfortabel ermöglicht. (...) es soll alles funktionieren (...) zu dem aber auch derjenige, der auf die Sicherheit schaut. Und es hat da natürlich Interessenskonflikte gegeben. Das ist natürlich sehr schwierig. Dadurch auch der eindringliche Appell an die Geschäftsführung, die das dann aber auch letztendlich umgesetzt haben, und das als Stabsstelle Informationssicherheit etabliert haben und die ISO-Rolle als Alleinstellungsmerkmal in das Unternehmen gebracht haben."* (Interview 1: 15-16)

Lediglich ein CISO, der auch gleichzeitig Leiter der IT-Abteilung ist, berichtet von keinen Konflikten mit der Geschäftsführung und Abteilungen, da er einerseits sehr lange im Unternehmen tätig ist und andererseits mit seiner Funktion als Leiter der IT-Abteilung sehr früh in neue Projekte involviert ist und hier sehr stark die Sicherheitsperspektive erbringen kann.

Ein Sicherheitsverantwortlicher berichtete über Konflikte mit der Mutterorganisation, die dadurch entstanden sind, weil die Tochterorganisation zum Teil die IT-Infrastruktur der Mutterorganisation verwendet, die zwar eine eigene Sicherheitsabteilung hat, aber aufgrund der Besonderheit des Unternehmens keine anfälligen Strafzahlungen nach der Datenschutz-Grundverordnung (DSGVO) zahlen muss. Das Tochterunternehmen muss hingegen sehr wohl Strafzahlungen bei Vergehen in Bezug auf die DSGVO leisten. Durch diese Firmenpolitik werden nur sehr sporadisch Informationen über Angriffe weitergeleitet.

Andere ExpertInnen berichteten auch von der gleichen Problematik, dass nur wenig Informationen zu Angriffen innerhalb der Unternehmensstruktur weitergegeben werden.

Bis auf zwei ExpertInnen berichten alle über eine positive Haltung der Geschäftsführung gegenüber den Sicherheitsmaßnahmen und den daraus resultierenden Einschränkungen, auch wenn Sicherheit in KMU´s nicht immer ernst genommen wird, was eher Budgetgründen zuzuschreiben ist.

Eine Behinderung der Prozesse durch Sicherheitseinschränkungen wird vielmehr von den Abteilungs- und Fachbereichsleitern als starke Einschränkung und Belastung empfunden, was nur durch breite Überzeugungsarbeit abgeschwächt werden kann.

Weitere Konflikte aufgrund der Doppelfunktion mit der IT-Leitung entstehen, wenn Sicherheitsmaßnahmen vom verfügbaren Budget der IT-Abteilung bzw. IT-Infrastruktur finanziert werden, welches in den meisten Unternehmen durch die hohen Kosten der kontinuierlichen Erneuerung der Infrastruktur und des Services stark belastet wird.

Keines der Unternehmen ist im Besitz einer Zertifizierung eines ISMS. Wobei von allen berichtet wurde, sich stark an der ISO Norm 27001 und den BSI Grundschutz anzulehnen und ein angepasstes ISMS in den nächsten Jahren umgesetzt wird.

5.4 Kategorie 4: Schulungsangebot im Unternehmen

Die ExpertInnen wurden über das derzeitige Angebot von Sicherheitsschulungen in ihren Unternehmen befragt. 85 codierte Segmente wurden in fünf Unterkategorien zugeordnet (Tabelle 9).

Schulungsangebot im Unternehmen
• Theorie-Schulung
• Häufigkeit und regelmäßige Aktualisierungen
• Verpflichtende Schulungen und Abschlussquizz

• Praktische Schulungen und Penetrationstests
• Handlungsempfehlungen für Sicherheitsschulungen

Tabelle 9: Kategorie 4 mit Unterkategorien

5.4.1 Theorie-Schulung

Theoretische Schulungen in Form von Online-Unterricht bzw. E-Learning-Programmen werden zum Zeitpunkt der Interviews in sieben von acht Unternehmen durchgeführt, um deren Personal in Bezug auf Informationssicherheit zu schulen. In einem Unternehmen existiert keine dezidierte Mitarbeiterschulung. Hier werden die Mitarbeitenden kontinuierlich mit relevanten Informationen zur allgemeinen Bedrohungslage und zu Awarenessmaßnahmen über ein Ticketsystem aufgeklärt.

Das Thema Social Engineering wird bei allen theoretischen Schulungen behandelt, wobei hier Abweichungen feststellbar sind. Weitere Themenbereiche in den Schulungen werden der allgemeinen Informationssicherheit und der DSGVO zugeordnet.

Drei ExpertInnen berichteten von einer nur sehr rudimentären Behandlung von Social Engineering in den Schulungen, wobei sich der Fokus eher auf den Angriffsvektor E-Mail konzentriert. Die übrigen ExpertInnen informierten über eine sehr intensive Behandlung von Social Engineering in ihren theoretischen Schulungen.

5.4.2 Häufigkeit und regelmäßige Aktualisierungen der Sicherheitsschulung

Betreffend der Häufigkeit der Durchführung und regelmäßigen Aktualisierung dieser Schulungen mit neuen Informationen und Angriffsvektoren wurden sehr unterschiedliche Angaben gemacht. Großteils werden diese Schulungen jedoch iterativ in definierten Zeiträumen für die Mitarbeiter angeboten, auch wenn in manchen Fällen die Mutterorganisation zusätzliche vereinzelte Schulungen anbietet.

Eine regelmäßige Aktualisierung der Schulungsprogramme wurde von vier ExpertInnen erwähnt, wobei alle ausdrücklich betonten, dass diese Schulungen erst kürzlich implementiert wurden. Bei den Übrigen wurden hauptsächlich Budgetgründe angegeben, warum die Schulungen teilweise sehr veraltet sind und nicht aktualisiert werden.

> *„Nein, also das Schulungsmaterial ist sicher nicht am aktuellen Stand. Das Material ist sicher älter als 5 Jahre und auch da wird die Notwendigkeit nicht gesehen, das Budget freizugeben."* (Interview 4, Pos. 60)

5.4.3 Verpflichtende Schulungen und Abschlussquizz

Bei der Hälfte der Unternehmen sind Mitarbeitende explizit verpflichtet, an der Sicherheitsschulung teilzunehmen. Unternehmensrichtlinien regeln die verpflichtende Durchführung der Schulung und unterrichten über den vorgegebenen Ablauf und Zeitrahmen der Absolvierung.

> *„E-Learning muss absolviert werden. Das Ergebnis wird an unsere globale Organisation gemeldet. Das heißt, es gibt da wirklich ein Reporting. Hundert Prozent der Belegschaft müssen dieses Programm bis zur Deadline durchgeführt und auch positiv beendet haben"* (Interview 3, Pos. 52)

Ein verpflichtender Abschlusstest wird nur in drei Unternehmen verlangt. Hier wurde von den ExpertInnen nach strengeren Richtlinien und Vorgaben von Seiten der Unternehmensleitung verlangt. Auch bei den Konsequenzen bei negativem Abschluss der Wissensüberprüfung oder unbegründeter Nichtdurchführung der Schulung fordern die Experten Handlungsbedarf.

Besonders die Unternehmensleitung könnte hier stärker Einfluss nehmen und Mitarbeitende auf dem direkten Weg über Konsequenzen unterrichten.

> *„Wir sind draufgekommen (...) es ist eine gute Sache, dass es von der Geschäftsführung kommitet wird und von der Geschäftsführung selbst der Mitarbeiter kontaktiert wird und auf die Schulung angesprochen wird. Das kommt anders an (...) höherer Druck, als wenn die Aufforderung vom ISO kommt. Das ist schon mal ein erster Schritt, um die Motivation der Teilnahme zu erhöhen. Es gibt aber keine Konsequenzen für besondere Spezialisten, die sich immer noch Zeit lassen."* (Interview 1: 81)

Zur Motivation der Belegschaft wurden in zwei Unternehmen Belohnungsmodelle implementiert. Bei erfolgreicher Absolvierung der Sicherheitsschulungen werden diverse Belohnungen verteilt, wie etwa Gutscheine, Teilnahme bei Gewinnspielen oder Tickets, die einzelne Mitarbeiterinnen und Mitarbeiter sowie auch ganze Abteilungen bei gutem Erfolg erhalten können. Durch die Gruppendynamik wird zusätzlich eine Triebkraft zur schnellstmöglichen und überdurchschnittlichen Ableistung der Sicherheitsschulung entwickelt.

5.4.4 Praktische Sicherheitsschulung und Penetrationstests

Praktische Sicherheitsschulungen werden kaum durchgeführt. Hier berichten die ExpertInnen von unterschiedlichen Ansätzen wie etwa die Veröffentlichung von Handouts, Plakaten und anderen Medien als Ersatz einer praktischen Sicherheitsschulung. Ein anderer Ansatz sind erweiterte modulartige theoretische Schulungen mit Praxisbezug für ausgewählte MitarbeiterInnen bzw. Rollen in verschiedenen sensiblen Bereichen, wie etwa für IT-Administratoren oder Führungskräfte.

In einem Unternehmen wurden interaktive, praktische Schulungen angeboten. Das Personal muss dabei verschiedene praktische Aufgaben lösen. Besonderes Hauptaugenmerk wird dabei auf Phishing und Spear-Phishing gesetzt, indem diverse Phishingkampagnen versendet und diese erkannt werden müssen.

In Verbindung mit Penetrationstests werden Angriffe, welche zuvor einvernehmlich mit dem Betriebsrat abgestimmt wurden, ausgerollt, um einerseits die Awareness des Personals messen zu können und andererseits der Belegschaft Rückmeldung über deren Verhalten geben zu können. Die Ergebnisse ermöglichen ein aktuelles Lagebild über das Sicherheitsbewusstsein der Mitarbeiter.

> *„Man kann alles konfigurieren und auch wenn der Mitarbeiter alles richtig gemacht hat, wird ihm alles angezeigt und in den E-Mail-Client integriert, wo der Mitarbeiter sämtliche Phishing-Mails mit einem Klick entsprechend behandeln kann. Er hat dann die Möglichkeit (...) er sieht irgendein Mail (...) Er weiß ja nicht, ob das eine Kampagne ist oder nicht.*

Er sieht einfach nur eine Phishing-Mail. Wenn es eine Kampagnen-Mail ist, bekommt er die Nachricht " Hast du gut gemacht" (Interview 1, Pos. 72)

„Es ist einerseits ein Awarenesstool für Mitarbeiter. Andererseits hilft es dem Unternehmen richtige Phishingkampagnen zu erkennen, weil mehrere Mitarbeiter in einem bestimmten Zeitraum bestimmte Mails weiterleiten, hat dann die Security Abteilung alles im Blick (...) Aha, da ist was im Laufen (...), sollte es der Spam-Filter nicht erkennen. Also es ist ein sehr durchdachtes Tool." (Interview 1, Pos. 73-74)

Bei einem zweiten Unternehmen sind ähnliche Maßnahmen in Planung. Grundsätzlich kann zusammengefasst werden, dass zurzeit nur unterdurchschnittlich wenig Unternehmen zusätzlich zu der theoretischen Schulung praktische Kurse bzw. Sicherheitsunterweisungen anbieten.

5.5 Kategorie 5: Handlungsempfehlungen der ExpertInnen

Diese Kategorie fasst die von den ExpertInnen aufgezeigten Handlungsempfehlungen zusammen, um daraus ableiten zu können. Bei den technischen Handlungsempfehlungen wurde auf jene abgegrenzt, die in unmittelbarer Verbindung zu organisatorischen Maßnahmen stehen.

Folgende Unterkategorien (Tabelle 10) wurden identifiziert.

Handlungsempfehlungen der ExpertInnen
• Handlungsempfehlungen zur Eingliederung des Sicherheitsverantwortlichen
• Handlungsempfehlungen für Sicherheitsschulungen und Penetrationstests
• Handlungsempfehlungen für die physische Sicherheit
• Handlungsempfehlungen für technische Schutzmaßnahmen

• Handlungsempfehlungen für organisatorische Schutzmaßnahmen

Tabelle 10: Kategorie 5 mit Unterkategorien

5.5.1 Handlungsempfehlungen zur Eingliederung des Sicherheitsverantwortlichen

Nach Auswertung der Ergebnisse wurde festgestellt, dass alle Interviewteilnehmer einstimmig angegeben haben, dass der/die Sicherheitsverantwortliche ausnahmslos direkt als Stabsstelle mit Weisungsrecht in der Unternehmensstruktur vollständig von den Abteilungen und Fachbereichen sowie allen operativen Aufgaben entkoppelt werden muss, da diese Funktion kontrollierende und regulatorische Aufgaben im Unternehmen erfüllen muss.

Idealerweise wäre der Security Officer somit als Stabsstelle der Gegenpol zum Chief Information Officer (CIO), da für den Sicherheitsverantwortlichen alle sicherheitsrelevanten Tätigkeiten im Vordergrund stehen, was auch die Digitalisierung und Modernisierung einschränken könnte.

> *„Klassischerweise gehört der Security-Officer nicht weisungsgebunden direkt unter die Geschäftsführung angesiedelt, weil das ja eigentlich ein Gegenpol ist zum CIO, weil der Security Officer ja auch Digitalisierung oder Modernisierung einschränkt."* (Interview 7: 15)

Zusätzlich müsse der Security Officer in die aktive Modellierung aller Geschäftsprozesse eingebunden werden. Dabei darf die Informationssicherheit nicht nur aus der Perspektive der IT betrachtet werden, sondern sollte in einen technischen-, organisatorischen- und personellen Bereich unterteilt und somit alle Geschäftsprozesse aus allen Perspektiven betrachtet und kontinuierlich evaluiert bzw. angepasst werden.

> *„Bis das soweit ist, (...) auch die Einbindung in alle Geschäftsprozesse (...) dauert das einfach. Weil es in den Köpfen noch nicht drinnen ist. Management sieht immer noch oft Informationssicherheit. (...) Das ist nur IT-Security".* (Interview 1, Pos. 43)

Doppelfunktionen wurden ebenfalls ausdrücklich abgelehnt, da viele weitgreifende Aufgabenbereiche Konflikte auslösen. Besonders die Leitung der IT-Abteilung wurde von allen als jene mit den meisten Interessenskonflikten angegeben.

Eine eigens für Sicherheit zuständige Person mit umfassenden IT- und Datenschutzkenntnissen ohne jeglicher Doppelfunktion, mit Weisungsrecht gegenüber den Abteilungen, wäre die induktiv abgeleitete Handlungsempfehlung von den interviewten ExpertInnen.

5.5.2 Handlungsempfehlungen für Sicherheitsschulungen und Penetrationstests

Die ExpertInnen für Informationssicherheit wurden unmittelbar im Anschluss an die Ausführungen betreffend Ist-Zustand und Angebot der Sicherheitsschulungen über mögliche Handlungsempfehlungen konsultiert. Die neuen Erkenntnisse zeigen, dass sich die ExpertInnen einen viel stärkeren Praxisbezug der Schulungen wünschen.

Ein möglicher stufenweiser Aufbau einer Sicherheitsschulung wäre demnach, eine individuelle theoretische Schulung für neu ins Unternehmen eingegliederte Mitarbeiter anzubieten, um eine gewisse Basis zu schaffen. Diese Basisschulung sollte in regelmäßigen Abständen verpflichtend von allen Mitarbeitenden absolviert werden. Diese theoretischen Schulungen sollten dem Personal Spaß machen und abwechslungsreich sein. Befürwortet wurde hier eine Alternation von Frontalvorträgen mit Onlinetools und Videos.

Ein Abschlusstest oder eine andere Form von Erfolgskontrolle wurde von den ExpertInnen eher abgelehnt, da dies das Personal abschreckt und das Bewusstsein für die verschiedensten Social Engineering Gefahren nicht steigert. Stattdessen wird eher ein Gamification[13]-Ansatz empfohlen. Mitarbeitende sollten sowohl bei theoretischen als auch bei praktischen Sicherheitsunterweisungen mit diversen Vergütungen belohnt werden.

[13] Anwendung spieltypischer Elemente

Bei den Konsequenzen im Falle wiederholter Nichtteilnahme an verpflichtenden Sicherheitsschulungen, ist die Haltung der InterviewteilnehmerInnen eher entschlossener. Hier empfehlen die ExpertInnen klare Konsequenzen durch Dienstanweisungen und Regelungen im Umgang mit der verpflichtenden Teilnahme an den Schulungen. Theoretische Schulungen müssen zudem ständig adaptiert werden und das Personal über Änderungen der Bedrohungslage über verschiedene Medien informiert werden.

Zusätzlich zu den theoretischen Schulungen sollte mehr Praxisbezug eingebaut werden. Ein Beispiel wären praktische Schulungen, wo Mitarbeitende durch diverse Hands-On Aktivitäten selber Angriffe erkennen bzw. Angriffskampagnen mithilfe von speziell dafür programmierten Tools durchführen.

Penetrationstests sind unterstützende Maßnahmen zur Messung der Sicherheit und des Verständnisses der Mitarbeiter in Bezug auf Social Engineering Angriffe. In Kombination mit Penetrationstests können den Mitarbeitenden anonymisiert die Ergebnisse dieser Test-Angriffe präsentiert werden, was das Bewusstsein über die Tricks erhöht und auch Einfachheit dieser Angriffe demonstriert. Das Personal darf diese Tests nicht als Überwachung kommunizieren. Ebenso dürfen auch einzelne nicht an den Pranger gestellt werden, wenn ein Test-Angriff erfolgreich durchgeführt wurde, da dies psychische oder gruppendynamische Auswirkungen haben könnte. Demzufolge ist es besonders wichtig, durch Überzeugungsarbeit und gute Kommunikation eine Akzeptanz für diese Testungen bei den Bediensteten zu erzeugen bzw. zu steigern.

Abschließend kann festgestellt werden, dass der Staat die Unternehmen bei der Durchführung von Awarenessmaßnahmen stärker unterstützen sollte. Besonders KMU´s haben weder die personellen noch finanziellen Ressourcen für die eigene Umsetzung von Sicherheitsschulungen oder die Auslagerung an externe Unternehmen und benötigen dahingehend bestmögliche Unterstützung von staatlicher Seite.

5.5.3 Handlungsempfehlungen für die physische Sicherheit

Für die physische Sicherheit im Unternehmen wird empfohlen, die Räumlichkeiten entsprechend ihrer Risiko-Klassifizierungsstufe in unterschiedliche Schutzzonen zu unterteilen, um den Zutritt von unbefugten Personen sehr stark zu erschweren. Speziell dafür konfigurierte elektronische Zutrittssysteme mit Zwei-Faktor Authentifizierung können Schutzzonen oder auch einzelne Räume wie etwa Serverräume absichern, welche durch qualifiziertes Personal kontinuierlich auf einwandfreie Funktionsweise zu prüfen sind.

> *„Die entsprechenden Räumlichkeiten mit unterschiedlichen Schutzzonen versehen und Serverräume anders abzusichern zusätzlich und vielleicht mit einem zweiten Faktor (…) "* (Interview 1: 111)

Eine zusätzliche Absicherung, unbefugte Personen identifizieren zu können, ist das verpflichtende Tragen von BesucherInnen- und MitarbeiterInnenausweisen.

5.5.4 Handlungsempfehlungen für technische Schutzmaßnahmen

Bei den in unmittelbarer Verbindung zu den organisatorischen Schutzmaßnahmen stehenden technischen Schutzmaßnahmen empfehlen die ExperteInnen hauptsächlich Verschlüsselungssysteme bzw. elektronische Signaturen für den E-Mail-Verkehr einzusetzen. Durch elektronische Signaturen kann das Schutzziel der Authentifizierung gewährleistet und die Gefahr eines E-Mail-Verkehrs mit einer unbefugten Person minimiert werden.

Die Trennung der physischen Netze verhindert grundsätzlich die Verbreitung von Schadsoftware innerhalb der Unternehmensnetzwerke. Hier kann evaluiert werden, ob auch der E-Mail-Verkehr physisch von den übrigen Netzen getrennt werden kann.

Zusätzlich wurde empfohlen, BYOD stark einzuschränken und stattdessen Firmengeräte anzuschaffen, die mittels eines Managementsystems verwaltet werden können. Grundsätzlich müssen Server und Tools von geeignetem und gut ausgebildeten Personal kontinuierlich verwaltet werden.

„Das sehen wir immer wieder in der täglichen Arbeit, dass Tools, die angeschafft werden (...) super sind und das Management glaubt dann,(...) ja toll, wir haben das Tool gekauft und somit sind wir safe. Nein! Das Tool ist eigentlich nur der kleinste Teil von dem Ganzen. Die Pflege des Tools und die Konfiguration des Tools (...) dass ist eigentlich die Hauptarbeit." (Interview 1: 116)

5.5.5 Handlungsempfehlungen für organisatorische Schutzmaßnahmen

Als eine der wichtigsten organisatorischen Schutzmaßnahmen wurde von den ExpertInnen eine Form von positiver Fehlerkultur beschrieben, bei der Mitarbeitende keine Repressalien bei Fehlern fürchten müssen. Durch offene Kommunikation mit anderen Mitarbeitenden und Information kann ein Berichtsweg im Unternehmen etabliert werden. Durch einen eindeutig definierten Dienstweg erhält der Sicherheitsverantwortliche oder CISO ein aktuelles Lagebild und kann versuchen, sofort Abwehrmaßnahmen bei Angriffskampagnen zu setzten.

Eine weitere organisatorische Maßnahme, die zur Implementierung im Unternehmen empfohlen wird, ist die Verlautbarung von Unternehmensrichtlinien über das Verhalten bei Sicherheitsvorfällen.

Eine Dienstanweisung von Seiten der Geschäftsführung wird hier ausdrücklich befürwortet, da dies von der Belegschaft konsequenter aufgenommen wird als eine Empfehlung von Sicherheitsrichtlinien, die von der IT-Abteilung verfasst und versendet wurde.

„Wie verhalte ich mich richtig. Das wäre eine sehr wichtige organisatorische Maßnahme, die auch von der Geschäftsführung als Richtlinie rausgegeben wird. Nicht irgendein Papier das ein IT-Betriebsmitarbeiter per Mail verschickt. Weil das oft bei uns zumindest einen Unterschied macht, ob das die Geschäftsführung absegnet (...) ob das in Form einer Dienstanweisung kommt, oder ob das wieder irgendein Papier oder irgendeine Mail ist, die irgendwer ausschickt." (Interview 1: 121)

Der Sicherheitsbeauftragte sollte alle Geschäftsprozesse kontinuierlich beurteilen, wie die Kommunikation zwischen den einzelnen Prozessschritten zu erfolgen hat.

Durch eindeutig festgelegte Kommunikationswege können Unachtsamkeiten verringert werden. Ebenso sollte begutachtet werden, wie der E-Mail-Verkehr zu externen Stakeholdern reduziert werden kann, um eines der kritischsten Einfallstore von Social Engineering Angriffen zu entschärfen. Eine Möglichkeit dazu bietet der Einsatz von vertrauenswürdigen Kommunikationsplattformen.

6 Beantwortung der Forschungsfrage und Schlussfolgerungen

In diesem Kapitel werden die Ergebnisse der empirischen Studie zusammengefasst und analysiert. Ziel dieses Kapitels ist es, die offene Forschungsfrage zu beantworten und durch Verdichtung von Wissen neue Theorien zu entwickeln. Folgende Forschungsfrage wurde im Rahmen dieser Publikation untersucht:

Aus welchen Gründen werden Unternehmen trotz umgesetzter Schulungsmaßnahmen Opfer von Social Engineering Attacken?

Folgende Schlussfolgerungen konnten aus den Ergebnissen der Expertengespräche und der Literaturstudie abgeleitet und zusammengefasst werden.

- Zunahme von gezielten Social Engineering Angriffen:

  Die Sicherheitsverantwortlichen meldeten eine starke Zunahme von Spear-Phishing Angriffen in den Unternehmen. Diese Angriffe werden auch immer ausgeklügelter ausgeführt und bedienen sich vieler neuer Technologien. Auch wenn E-Mails als größtes Einfallstor dieser Angriffe bezeichnet werden, nutzen die Angreifenden vermehrt Social Media Kanäle zum Sammeln von detaillierten Informationen ihrer Ziele und gleichzeitig zum Versenden von mit Schadsoftware behafteten Links und Nachrichten mit den in Social Media Kanälen integrierten Kurznachrichtendiensten.

  Ein besonders lukratives Ziel ist es, an die Zugangsdaten der Messenger zu gelangen und Angriffe innerhalb der MitarbeiterInnenkanäle, bei denen sich die User relativ sicher fühlen, zu starten. Zusätzliche neue Bedrohungen durch einfaches Reproduzieren von Daten durch Unterstützung von Künstlicher Intelligenz (KI) und dem Einsatz von realistisch wirkenden gefälschten Medieninhalten bringen viele neue Herausforderungen für Sicherheitsverantwortliche und Unternehmen, die bei diesen Abwehrmaßnahmen Trends nicht mithalten können.

- **Unzureichende Sicherheitsschulungen:**

Auch wenn in größeren Unternehmen bereits moderne Konzepte von verschiedenen Sicherheitsschulungen in den letzten Jahren implementiert wurden, besteht dringender Nachholbedarf bei einer ganzheitlichen Sicherheitsschulung. Keines der Unternehmen setzt Kennzahlenmodelle für die Awareness der Mitarbeitenden ein. Großteils berichteten die Experten von nicht kontinuierlich aktualisierten Schulungsinhalten. Praktische Sicherheitsschulungen werden so gut wie keine eingesetzt.

Die zuvor beschriebene Zunahme von gezielten Social Engineering Angriffen und der Einsatz neuer Technologien erfordert praktische Schulungsmaßnahmen, bei denen Teilnehmer durch Rollenspiele, Sammeln von Informationen durch Open Source Intelligence[14] (OSINT) und selbst erstellte Angriffskampagnen die Angriffsmethoden besser verstehen und dadurch besser abwehren können.

- Wenig Akzeptanz bei Sicherheitsmaßnahmen in KMU`s:

Für Sicherheitsmaßnahmen fehlt im Gegensatz zu großen Unternehmen in KMU´s der Geschäftswert und das Verständnis der oft sehr patriarchalen Firmenstrukturen. Der Kostenfaktor ist das wichtigste Entscheidungskriterium. Sicherheit hat in KMU´s keine Priorität.

- Doppelfunktionen von Sicherheitsverantwortlichen:

Sechs der insgesamt acht interviewten ExpertInnen bekleiden eine Doppelfunktion in ihren Unternehmen. Besonders die gleichzeitige Rolle des IT-Leiters sorgt für viele Interessenskonflikte im Unternehmen, insbesondere aus Budgetgründen, fehlender Akzeptanz und Widerstand bei den in der Organisationsstruktur gleich abgebildeten Abteilungen.

[14] Nachrichtengewinnung durch frei verfügbare Quellen

- CISO nicht als Stabsstelle in den Unternehmen eingegliedert:

Die dezidierte Rolle des CISO wird in vielen Unternehmen nicht anerkannt. Die Rolle des Informationssicherheitsverantwortlichen wird oft mit der des Datenschutzbeauftragten gleichgestellt. Aufgrund der fehlenden Befugnisse im Unternehmen hat sie keinen Einfluss auf die Anpassung der Geschäftsprozesse in Bezug auf die Sicherheitsmaßnahmen und keine Weisungsrechte gegenüber den Abteilungen und Mitarbeitenden.

- Fehlende Unternehmensrichtlinien für interne Kommunikation:

Die ExpertInnen berichteten von Konflikten in der Holdingstruktur, insbesondere bei Weiterleitung von sicherheitsrelevanten Informationen der Mutterorganisation zu deren Tochterunternehmen und der Bildung von Barrieren bei den Sicherheitsverantwortlichen durch Firmenpolitik.

Ebenso fehlen Richtlinien für interne Kommunikationswege von der Belegschaft zu den Sicherheitsverantwortlichen bei Verdacht oder Tatbestand eines Angriffes auf die Informationssicherheit.

7 Organisatorische Handlungsempfehlungen

Nach Auswertung und Diskussion der Ergebnisse wurden organisatorische Handlungsempfehlungen für Schutzmaßnahmen für Unternehmen und Organisationen abgeleitet. Als Grundlage und zur Gliederung der Problemstellungen und daraus abgeleiteten Handlungsempfehlungen wurden die aus Kapitel 6 präzisierten Ergebnisse jeweils als eigenständige Probleme interpretiert, aus denen mögliche Handlungsempfehlungen zur Minimierung von Social Engineering Angriffen entwickelt wurden.

Diese Handlungsempfehlungen wurden aus der Theorierecherche (Kapitel 3 Stand des Wissens) und den Ergebnissen der Expertengespräche zu neuen Theorien generiert. Die berufliche Erfahrung des Autors in Bezug auf Informationssicherheit und das erlangte Fachwissen durch umfangreiche Untersuchungen zu dieser Thematik und Problematik wurden zusätzlich zur Begründung dieser Handlungsempfehlungen eingesetzt.

7.1 Informationssicherheitsbeauftragter im Unternehmen

BetreiberInnen einer kritischen Infrastruktur wie etwa im Finanz- Energie oder Gesundheitswesen sind gesetzlich dazu verpflichtet, ein effektives Informationssicherheitsmanagementsystem (ISMS) im Unternehmen zu implementieren. Auch in vielen großen Unternehmen hat sich ein ISMS bereits etabliert, wenn auch noch mit vielen Lücken und Schwierigkeiten. Das fehlende Budget der Sicherheitsstabstellen und der Mangel an qualifizierten Arbeitskräften in dieser Branche, insbesondere in staatlichen Organisationen, haben starke Auswirkungen auf die Sicherheitskultur in den Unternehmen.

Die Implementierung eines ISMS ist somit auch für staatliche Organisationen und große Unternehmen ein sehr schwieriges Unterfangen. Für KMU´s gestaltet sich der Aufbau eines wirksamen und kontinuierlich modifizierbaren ISMS durch die Komplexität und Kostspieligkeit als beinahe unmöglich. Ein ganzheitlicher Ansatz eines etablierten Sicherheitskonzepts mit den dafür notwendigen Rollen und Prozessen, hat sich nur selten in Unternehmen aller Betriebsgrößen durchgesetzt. Sehr oft ist die Abgrenzung

der unterschiedlichen Funktionen in der IT-Sicherheit nicht eindeutig, sodass abweichende Bezeichnungen der Rollen in den Unternehmen verwendet werden.

Luber (2017) beschreibt den CISO als Chief Information Security Officer. Dem Hauptverantwortlichen für Informationssicherheit im Unternehmen, dessen Position grundsätzlich als Bestandteil der Geschäftsführung dem Chief Executive Officer (CEO) berichtet und nur dieser weisungsbefugt gegenüber dem CISO sein soll (Luber, 2017).

Trotz der unterschiedlichen Arbeitstitel des Sicherheitsverantwortlichen im Unternehmen ist in der Handlungsempfehlung aufgrund der Aussagen der ExpertInnen und der Literaturrecherche abzuleiten, dass die Funktion des Sicherheitsverantwortlichen unmittelbar von der Geschäftsführung als Stabsstelle mit Weisungsrecht gegenüber den Abteilungen ohne jeglicher Doppelfunktion zugeordnet sein muss.

7.2 Reifegradmodell für Informationssicherheit

Der Umsetzungsgrad der Informationssicherheit sollte analog zu Reifegradmodellen von Geschäftsprozessen modelliert werden. Ein Reifegradmodell hilft den Verantwortlichen bei der Einschätzung, Steuerung und kontinuierlichen Optimierung von Prozessen. Bei der strategischen Beurteilung für den Einsatz eines Reifegradmodells in der Informationssicherheit steht nicht wie bei einem Reifegradmodell im Prozessmanagement der Kundennutzen sowie die Wertschöpfungskette im Fokus, sondern die Informationssicherheit mit ihren drei Perspektiven (Abbildung 7.1). Zu der organisatorischen Perspektive werden Governance, Risikomanagement und Business Continuity Management (BCM) zugeordnet.

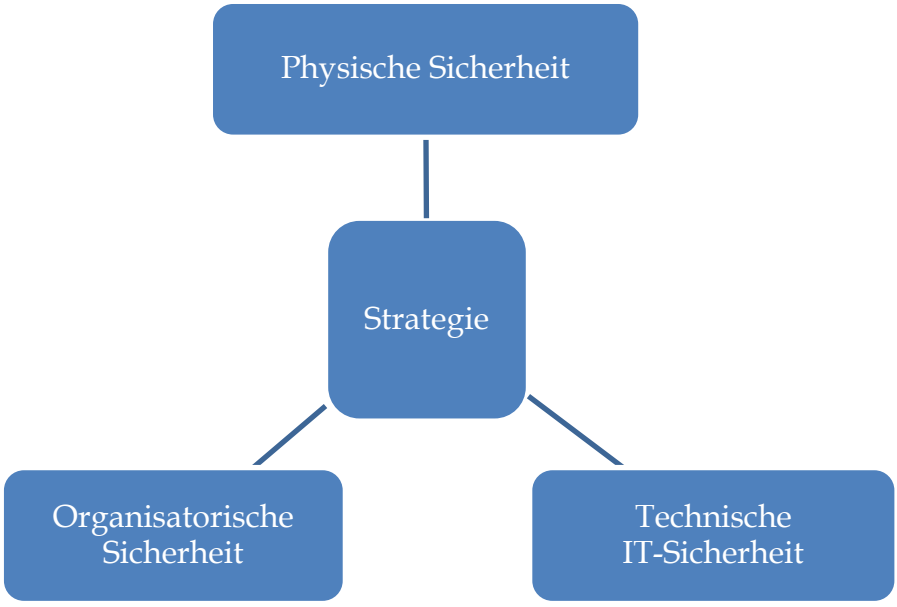

Abbildung 7.1: Perspektiven der Informationssicherheit (eigene Darstellung)

Das Bundesamt für Informationssicherheit (2021) beschreibt mögliche Reifegrade mit deren Merkmalen als Maßstab für ein ISMS (Abbildung 7.2).

Abbildung 7.2: Reifegradmodell für ISMS (in Anlehnung an Reifegradmodelle, 2021)

Ein wesentlicher Faktor ist das Messen der Prozessleistung. Key Performance Indikators (KPI) müssen zur Messung der Informationssicherheit von den Sicherheitsverantwortlichen definiert werden (Reifegradmodelle, 2021).

Die nachfolgende Abbildung 7.3 zeigt ein Beispiel einer Analyse der Teilbereiche eines ISMS durch ein Reifegradmodell. Damit kann graphisch illustriert werden, wo der Reifegrad niedrig ist und somit Handlungsbedarf besteht.

Abbildung 7.3: Auswertung durch das Reifegradmodell (Reifegradmodelle, 2021)

Eine Möglichkeit einer Kennzahl, die speziell für Social Engineering Angriffe konstruiert wurde, ist der "Employee Security Index (Kapitel 3.5.4).

Mit dieser Kennzahl können Basislinien definiert werden, die alle MitarbeiterInnen in einer gewissen Zeit erreichen bzw. aufrechterhalten müssen. Dies ist nur in Kombination mit theoretischen und praktischen Schulungsmaßnahmen sowie Penetrationstests möglich.

7.3 Schulungsmaßnahmen

Eine Kombination von theoretischen und praktischen Schulungsmaßnahmen für einen Aufbau von Security-Awareness ist für Unternehmen unumgänglich. Dieser Prozess muss bereits bei der Aufnahme von neuen Mitarbeitenden beginnen. Zielsetzung dieser Schulung muss die umfangreiche Wissensvermittlung von Gefahren in Bezug auf Social Engineering und andere Angriffsmethoden sein, um einen definierten Reifegrad zur Informationssicherheit zu erreichen und das Risiko von erfolgreichen Angriffen stark minimieren zu können.

Das Hauptaugenmerk darf dabei nicht nur auf den Schutz der Informationen im Unternehmen liegen, sondern auch ein Verständnis für die Gefahren dieser Angriffsart zu entwickeln, die Mitarbeitende auch in den eigenen vier Wänden angreifbar macht. Dazu gehört auch der verantwortungsbewusste Umgang mit Social Media Plattformen, insbesondere jene zur Pflege von Geschäftskontakten bzw. Jobbörsen wie LinkedIn, wo nicht selten der gesamte Lebenslauf der Person und andere sensible Daten hochgeladen werden.

Ein zur Zeit der Verfassung dieser Publikation erfolgter Datenmissbrauch von 500 Millionen LinkedIn-Konten, inklusive aller darin enthaltenen personenbezogenen Daten, zeigt, wie verletzlich Menschen durch den Missbrauch von persönlichen Daten werden können (Vanian, 2021).

Viele Unternehmen unterscheiden hier bei der Klassifizierung des Arbeitsplatzes zwischen den Schutzzielen und dem Zugang zu Informationen und Tätigkeiten, die nach erfolgter Risikoanalyse zugeteilt werden. Somit werden oft die Inhalte der Sicherheitsschulung an den jeweiligen Arbeitsplatz bzw. Berufsgruppe im Unternehmen angepasst indem suggeriert wird, dass Personen mit Zugang zu besonders klassifizierten Informationen und Tätigkeiten ein großes Sicherheitsrisiko darstellen.

Besonders bei dieser Herangehensweise steckt die Gefahr im Detail. AngreiferInnen suchen sich die sogenannte „schwächste Stelle der Informationssicherheit“ aus. Das sind meistens Personen, die nicht zwingend Zugang zu besonders schützenswerten Informationen haben, aber indirekt an Daten gelangen können. Das können etwa Reinigungsfachkräfte, Hilfspersonal oder Auszubildende im Sekretariat sein.

Aus diesem Grund ist zu empfehlen, bei den Inhalten und dem Umfang der Sicherheitsschulung nicht zwischen Rollen und Tätigkeiten sowie Klassifizierungsstufen zu unterscheiden, sondern dasselbe Awareness-Training, welches aus einem theoretischen Basisteil und einer praktischen Schulung besteht, für alle Mitarbeiter einzusetzen.

7.3.1 Basisschulung

Durch Unterstützung von an die Erfordernisse der Unternehmen anpassbare Online-Schulungsprogramme können Unternehmen eine theoretische Grundlage für Mitarbeiter schaffen, was besonders beim individuellen Onboarding Prozess von neuen Mitarbeitern Kosten einsparen würde. Dies wird durch den geringen Personaleinsatz bei Einsatz eines automatisierten Schulungsprogrammes sichergestellt, da neue Mitarbeiter diese Schulungen selbständig ausführen können. Folgende theoretische Inhalte (Kapitel 3.3) zum Erreichen einer Basis-Awareness für Social Engineering sollten in der Basisschulung enthalten sein.

- Phishing
- Spear-Phishing
- Unterschiede der einzelnen Unterkategorien von Phishing und Spear- Phishing
- Quid pro Quo Attacken
- Tailgaiting

Durch eine Wissensüberprüfung am Ende jeder Einheit kann festgestellt werden, ob der Mitarbeiter die Inhalte auch verstanden hat. Das Hauptaugenmerk der Prüfung sollte die eindeutige Identifizierung von Social Engineering Angriffen sein. Praktische Vorlagen von realen Beispielen können dabei unterstützen.

Hier ist darauf zu achten, dass das Ergebnis der Wissensüberprüfung nur an den Sicherheitsverantwortlichen weitergeleitet wird und der Mitarbeitende die Überprüfung beliebig oft durchführen kann. Erst bei mehrmaliger negativer Überprüfung kann eine persönliche Unterstützung und Hilfestellung durch den eingeteilten Sicherheitsverantwortlichen des Unternehmens erfolgen.

Nach erfolgter Wissensüberprüfung wird eine Basislinie erreicht, die zuvor im Reifegradmodell und der Kennzahl exakt definiert wurde. Abbildung 7.4 zeigt den erreichten Basislevel gestützt auf die Kennzahl „Employee Security Index“ (Kapitel 3.5.4). Bei diesem Beispiel wird nach Überschreiten des kritischen Wertes der akzeptable Bereich (Basis) erreicht.

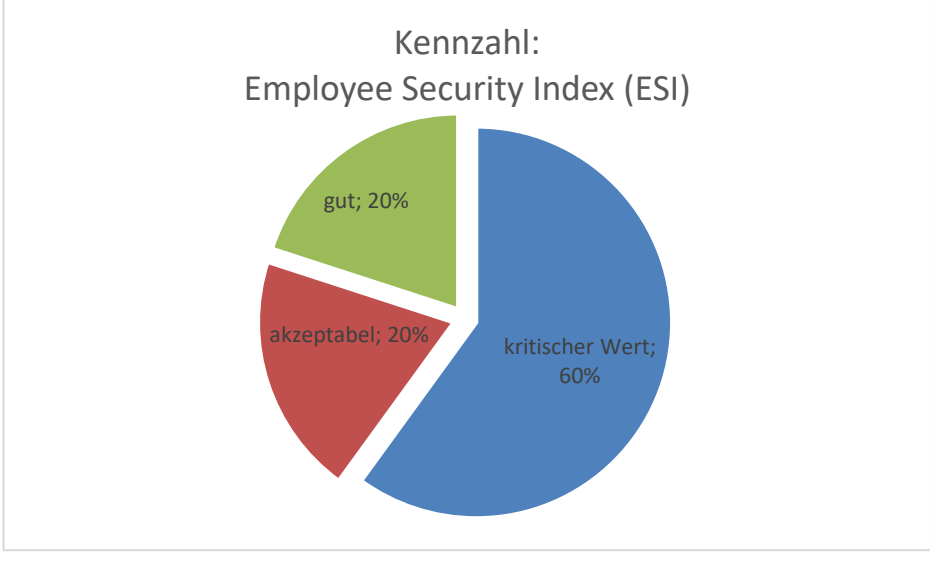

Abbildung 7.4: Beispiel für die Kennzahl ESI (eigene Abbildung)

Es wird empfohlen diese Schulung innerhalb eines bestimmten Zeitraumes, jedoch mindestens jährlich zu wiederholen.

Die Inhalte müssen iterativ an die aktuelle Lagesituation angepasst werden. Wenn ein Mitarbeiter in dem vorgegebenen Zeitraum die Schulung nicht absolviert, wechselt die individuelle Kennzahl wieder in den kritischen Bereich. Mögliche Konsequenzen müssen dringend von Seiten der Geschäftsführung durch eine Dienstanweisung definiert werden.

Mögliche Inhalte dieser Dienstanweisung können etwa die Definition von Zeiträumen für Nachfristen, oder die Sperre von Rollenrechten als letzte Konsequenz und der Verlust des Zuganges zu klassifizierten Informationen sein

7.3.2 Erweiterte praktische Schulung

Immer besser werdende ausgeklügelte Social Engineering Angriffe sind nur sehr schwer für ungeschulte Personen zu erkennen. Bei der Implementierung von praktischen Schulungen besteht dringender Handlungsbedarf in Unternehmen und Organisationen aller Betriebsgrößen. Praktische Schulungen bilden eine Erweiterung der theoretischen Sicherheitschulungen. Durch Einsatz von Rollenspielen, die durch qualifiziertes Personal erstellt und überwacht werden, können reale Angriffsszenarien in der natürlichen Umgebung (Firmengelände, Gebäude) nachgespielt werden und so die Awareness signifikant steigern.

Besonders klassische Social Engineering Angriffe wie Tailgaiting oder Vishing können mit dieser Form des Szenarientrainings durchgeführt werden.

Nachfolgend werden verschiedene Angriffsszenarien und mögliche Inhalte der praktischen Sicherheitsschulung beschrieben.

- Angriffsvorbereitung:

  Ziel dieses Schulungsteiles ist die Vorgangsweise der Angreifenden besser verstehen zu können und sensibler mit Social Media Informationen umzugehen.

Dafür werden OSINT-Tools und Social Media Suchmaschinen genutzt, um möglichst viele offene Informationen über Zielpersonen (fiktive Personen) zu finden.

Durch die Analyse der Ergebnisse können mögliche Schwachstellen der Opfer und Angriffsmethoden abgeleitet werden.

- Phishing und Spear-Phishing:

Mit dem Einsatz von Phishing-Tools können realitätsnahe Angriffskampagnen an die Gegebenheiten und Kommunikationsstrukturen der jeweiligen Unternehmen angepasst und ausgerollt werden. Mitarbeitende müssen im Zuge dieser Ausbildung Angriffe von echter Korrespondenz unterscheiden. Die Awareness kann besonders gesteigert werden, wenn Mitarbeitende selbst in einer Laborumgebung (eigenes Übungsnetzwerk) Phishing und Spear-Phishing Angriffe erstellen und so die Vorgangsweise der Angreifenden besser verstehen können. Insbesondere die Tatsache wie einfach durch moderne Tools ohne besonderes IT-Fachwissen Daten reproduziert werden können, wie in Abbildung 3.5 bereits dargestellt wurde.

- Vishing:

Bei diesem Ausbildungsteil können Rollenspiele in Form von Telefonanrufen durchgeführt werden. Von den Teilnehmenden kann versucht werden, sensible Daten von Mitarbeitenden, KundenInnen, LieferantInnen oder sonstigen Stakeholdern zu erfragen. Zeitdruck oder Drohungen helfen den Angreifern bei ihren Zielpersonen unüberlegte Handlungen zu erzwingen.

Weitere Möglichkeiten für praktische Beispiele kann das unbefugte Eindringen in das Firmengebäude über einen Notausgang sein, oder durch Tarnung (Servicekleidung der Druckerfirma oder eines Lieferanten) in sensible Unternehmensbereiche zu gelangen.

7.4 Penetrationstests

Mit gezielten Penetrationstests auf IKT-Systeme und MitarbeiterInnen können Dienstgeber den aktuellen Zustand der technischen Abwehrsysteme und die Awareness der Mitarbeitenden testen. Die Ergebnisse unterstützen den Sicherheitsverantwortlichen bei der Planung und Durchführung von Schulungsmaßnahmen. Zusätzlich sollten die gemessenen Werte in die Kennzahl „Employee Security Index" eingebettet werden.

Für die Durchführung von Penetrationstests wird empfohlen an externe Anbieter outsourcen zu lassen, um ein unvoreingenommenes Lagebild für den Sicherheitsverantwortlichen zu schaffen. Besonders wichtig für die Vorgehensweise ist es, den Mitarbeitern nicht das Gefühl zu geben überwacht zu werden. Dazu sind informierende Gespräche mit den Mitarbeitenden und der ArbeitnehmerInnenvertretung sowie rechtliche Absicherung notwendig. Je nach Komplexität sollten diese Penetrationstests regelmäßig ausgeführt werden, um auch den Fortschritt bei der MitarbeiterInnen-Awareness messen zu können.

7.5 Mapping von Geschäftsprozessen

Business Process Mapping ist ein wesentlicher Baustein bei der kontinuierlichen Überwachung und Verbesserung der Geschäftsprozesse. Sicherheitsverantwortliche sollten die Prozessabbilder in Bezug auf Social Engineering Angriffsvektoren evaluieren. Eine erneute Überprüfung bei jeder Prozessänderung ist für die kontinuierliche Überwachung der Sicherheitsaspekte dringend notwendig. Mögliche sicherheitsrelevante Faktoren der Prozessabbildungen sind:

- Informationen
- alle am Prozess beteiligten Rollen
- alle Interaktionen

Voraussetzung für die Durchführung von Business Process Mapping ist der Einsatz von strategischem Geschäftsprozessmanagement im Unternehmen.

8 Zusammenfassung und Ausblick

In diesem Kapitel werden die Ergebnisse dieser Publikation zusammengefasst. Abschließend wird ein Ausblick über zukünftige Herausforderung von Social Engineering und weiterführende Vorschläge für Untersuchungen zu diesem Forschungsgegenstand vorgestellt.

8.1 Zusammenfassung der Erkenntnisse

In dieser Publikation wurde analysiert, warum Unternehmen aller Betriebsgrößen trotz implementierter Schulungsmaßnahmen Opfer von Social Engineering Angriffen werden. Nach der Einleitung in die Thematik und Erläuterung der Problemstellung wurde zunächst angenommen, dass Sicherheitsschulungen zur Prävention von Social Engineering Angriffen in den Unternehmen angesichts der zahlreichen Angriffe und weltweiten Schäden in Milliardenhöhe evaluiert und neue Ansätze von Schutzmaßnahmen entwickelt werden müssen.

Die spärlich vorhandene Primärliteratur zu dieser Problemstellung begründete die Auswahl des qualitativen Forschungsprozesses zur Beantwortung der offenen Forschungsfrage. Zur Datenerhebung wurden leitfadengestützte ExpertInneninterviews mit acht Informationssicherheits-experten durchgeführt. Die erhobenen Daten wurden anschließend mittels der strukturierten, qualitativen Inhaltsanalyse nach Mayring ausgewertet und interpretiert.

Die Ergebnisse und Beantwortung der Forschungsfrage zeigen, dass dringender Handlungsbedarf bei der organisatorischen Struktur und den Befugnissen der Sicherheitsverantwortlichen besteht, da diese oft mit Doppelfunktionen im operativen Betrieb ohne Weisungsbefugnisse gegenüber den Abteilungen in den Unternehmen eingegliedert sind. Konflikte innerhalb der Unternehmen sowie mit der Mutter- bzw. den Tochterunternehmen in Bezug auf die Informationssicherheit resultieren aus konkurrierenden Sicherheits-verantwortlichen mit unterschiedlichen Befugnissen und Handlungsfreiheiten.

Zusätzlich wurde erforscht, dass aufgrund der steigenden Bedrohung von immer ausgeklügelten Social Engineering Angriffen die Akzeptanz und Awareness der MitarbeiterInnen durch zusätzliche Schulungsmaßnahmen unter Einsatz von praktischen Sicherheitsschulungen gesteigert werden müssen, um die Risiken von erfolgreichen Social Engineering Angriffen drastisch senken zu können. Nach Analyse der Ergebnisse wurden Handlungsempfehlungen zur Implementierung einer ganzheitlichen Sicherheitskultur für Unternehmen aller Betriebsgrößen abgeleitet.

8.2 Ausblick für zukünftige Forschung

Die Forschungsergebnisse dieser Publikation gewähren Einblick in die Problematik von Social Engineering Angriffen. Besonders die Einsicht über unvorteilhafte Eingliederung der Sicherheitsverantwortlichen und kontinuierliche Bereitstellung von theoretischen sowie praktischen Schulungen und die Etablierung einer offenen Fehlerkultur können Unternehmen für zukünftige organisatorische Schutzmaßnahmen nutzen.

Vieles hat sich durch die Covid-19 Pandemie geändert. Kollaboratives Arbeiten im Homeoffice und Technologien, die diese Form der verteilten Arbeitsumgebungen ermöglichen, stellen SicherheitsexpertInnen vor viele neue Herausforderungen. Geschäftsanforderungen müssen regelmäßig an Sicherheitsvorgaben angepasst werden, um Bedrohungen erkennen und abwehren zu können. Die Geschäftsführung und Sicherheits-verantwortlichen sind hier verantwortlich, bestmöglichen Schutz des Unternehmens und der MitarbeiterInnen gewährleisten zu können.

Immer moderner werdende Social Engineering Angriffe ermöglichen Schadsoftware über Social Media Kanäle und Kurznachrichtendienste verschleiert zu senden. Besonderes Hauptaugenmerk zukünftiger Forschungen sollte auf die Erkennung bzw. Prävention von technischen Schutzmaßnahmen und angepasste Risikoanalysen gelegt werden.

Für die Sicherstellung einer adaptiven Sicherheit gehört zusätzlich ein an das Unternehmen angepasstes Business Continuity Management (BCM). Es existieren viele Frameworks für BCM.

Trotzdem scheitern unzählige Sicherheitsverantwortliche an der Umsetzung, was hauptsächlich auf das Unverständnis der Geschäftsführung und Organisationsleitung zurückzuführen ist. Eine ganzheitliche Denkweise kann Sicherheitsverantwortliche bei der Einrichtung einer sicheren Arbeitsumgebung unterstützen. Dabei müssen folgende Komponenten berücksichtigt werden:

- Faktor Mensch
- Netzwerksicherheit
- Sichere Zusammenarbeit mit Kollaborations-Tools
- Sichere Arbeitsumgebung

Abschließend wird empfohlen, dass zukünftigen Forschungen im Bereich der Informationssicherheit ihren Fokus auf alle Elemente der adaptiven Sicherheit setzen.

9 Literatur

Aldawood, H. (2019). Challenges of Implementing Training and Awareness Programs Targeting Cyber Security Social Engineering. *Cybersecurity and Cyberforensics Conference*.

Alharthi, D., & Regan, A. (2021). Social Engineering Infosec Policies (SE-IPS). *Computer Science & Information Technology (CS & IT)*, 57–74. https://doi.org/10.5121/csit.2021.110104

Anand, A. (2019). *Preventing contact centre IVR fraud | UK Finance*. https://www.ukfinance.org.uk/news-and-insight/blogs/preventing-contact-centre-ivr-fraud

Anleitung zur Migration von Sicherheitskonzepten. (2018). Bundesamt für Sicherheit in der Informationstechnik.

Beckers, K., Schosser, D., Pape, S., & Schaab, P. (2017). A Structured Comparison of Social Engineering Intelligence Gathering Tools. In J. Lopez, S. Fischer-Hübner, & C. Lambrinoudakis (Hrsg.), *Trust, Privacy and Security in Digital Business* (Bd. 10442, S. 232–246). Springer International Publishing. https://doi.org/10.1007/978-3-319-64483-7_15

Beißel, S. (2017). Differenzierung von Rahmenwerken des IT-Risikomanagements. *HMD Praxis der Wirtschaftsinformatik*, *54*(1), 37–54. https://doi.org/10.1365/s40702-016-0281-2

Bischof, D. (2020). *Spionagefall im Bundesheer: „Das erinnert an Oberst Redl“*. Österreich Politik - Nachrichten - Wiener Zeitung Online. https://www.wienerzeitung.at/nachrichten/politik/oesterreich/2083782-Das-erinnert-an-den-Oberst-Redl.html

Bisson, D. (2019). *5 Social Engineering Attacks to Watch Out For*. https://www.tripwire.com/state-of-security/security-awareness/5-social-engineering-attacks-to-watch-out-for/

Böhl, L. (2020). *Pretexting (Definition und Schutzmaßnahmen)*. stuttgarter-nachrichten.de. https://www.stuttgarter-nachrichten.de/inhalt.pretexting-definition-mhsd.b2e3d060-f345-43e3-8541-6544e00c7ada.html

Brandt, Ma. (2016). *Infografik: Cyberattacken meist Insider-Jobs*. Statista Infografiken. https://de.statista.com/infografik/5001/verursacher-von-cyberattacken-auf-unternehmen/

Brüsemeister, T. (2008). *Qualitative Forschung: Ein Überblick* (2., überarb. Aufl). VS, Verl. für Sozialwiss.

BSI - G 0 Elementare Gefährdungen—IT-Grundschutz-Kataloge—G 0.42 Social Engineering. (2011). Bundesamt für Sicherheit in der Informationstechnik. https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/g/g00/g00042.html;jsessionid=988A43F34FD498D6BB89B4371E7F3CFF.1_cid341

BSI - IT-Grundschutz-Kompendium—1 IT-Grundschutz – Basis für Informationssicherheit. (2020). https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKompendium/vorkapitel/1_IT-Grundschutz_%E2%80%93_Basis_f%C3%BCr_Informationssicherheit.html

BSI - IT-Grundschutz-Standards. (2020). https://www.onlinesicherheit.gv.at/Themen/Experteninformation/Normen-und-Standards/BSI-IT-Grundschutz-Standards.html

BSI für Bürger—Informationen—Vorsicht Phishing: Die Corona-Krise als Köder. (2020). BSI. https://www.bsi-fuer-buerger.de/BSIFB/DE/Service/Aktuell/Informationen/Artikel/phishing-corona.html

BSI IT Grundschutz vs. ISO 27001—Iso-27001.at. (2020). https://www.iso-27001.at/bsi-it-grundschutz-vs-iso-27001/

Bullée, J.-W. H., Montoya, L., Pieters, W., Junger, M., & Hartel, P. (2018). On the anatomy of social engineering attacks-A literature-based dissection of successful attacks: On the anatomy of social engineering attacks. *Journal of Investigative Psychology and Offender Profiling*, *15*(1), 20–45. https://doi.org/10.1002/jip.1482

Calixto, E. (2016). *Gas and oil reliability engineering: Modeling and analysis* (2nd edition). Elsevier.

Chapple, M., & Seidl, D. (2019). *Exploiting Physical and Social Vulnerabilities*. Wiley.

Cyber Actors Take Advantage of COVID-19 Pandemic to Exploit Increased Use of Virtual Environments. (2020). FBI. https://www.ic3.gov/Media/Y2020/PSA200401

Cyber Defence News. (2020). it-daily.net. https://www.it-daily.net/it-sicherheit/cybercrime/23886-watering-hole-attacke-holy-water-identifiziert

Datenschutz, datensicherheit de I. zu D. und. (2021). *Finn der Fuchs: Kindern spielerisch IT-Sicherheit vermitteln*. datensicherheit.de Informationen zu Datensicherheit und Datenschutz. https://www.datensicherheit.de/finn-fuchs-kinder-spiel-it-sicherheit-vermittlung

Decker, K. M. (2017). Informationssicherheit – ohne methodische Risikoidentifizierung ist alles Nichts. *HMD Praxis der Wirtschaftsinformatik*, *54*(1), 21–36. https://doi.org/10.1365/s40702-017-0288-3

Deistler, N., & Rentrop, C. (2020). IT-Compliance in KMU – State of the art. *HMD Praxis der Wirtschaftsinformatik*, *57*(5), 1047–1057. https://doi.org/10.1365/s40702-020-00612-z

Domainanbieter gaukelte Mitarbeitern Weihnachtsbonus vor und warnte dann vor Phishing. (2020). DER STANDARD. https://www.derstandard.at/story/2000122778813/domainanbieter-gaukelte-mitarbeitern-weihnachtsbonus-vor-und-warnte-dann-vor-phishing

Döring, N., & Bortz, J. (2016a). *Forschungsmethoden und Evaluation in den Sozial- und Humanwissenschaften* (5. vollständig überarbeitete, aktualisierte und erweiterte Auflage). Springer.

Döring, N., & Bortz, J. (2016b). *Forschungsmethoden und Evaluation in den Sozial- und Humanwissenschaften* (5. vollständig überarbeitete, aktualisierte und erweiterte Auflage). Springer.

Drechsler, D. (2019). *Schutz vor Social Engineering: Angriffspunkte und Abwehrmöglichkeiten in digitalwirtschaftlichen Ökosystemen*.

ENISA ETL Report 2020—Phishing (EN). (2020). ENISA.

Etzemüller, T., & Zentrum Für Zeithistorische Forschung Potsdam. (2017). Social engineering. *Docupedia-Zeitgeschichte*. https://doi.org/10.14765/ZZF.DOK.2.1112.V2

FACC-Betrug: Finanzvorständin muss gehen. (2016, Februar 3). https://futurezone.at/b2b/facc-betrug-finanzvorstaendin-muss-gehen/178.785.380

Field, M. (2019, Februar 20). NATO researchers used social media to learn details of a military exercise and manipulate troops. It wasn't very hard to do. *Bulletin of the Atomic Scientists*. https://thebulletin.org/2019/02/nato-researchers-used-social-media-to-learn-details-of-a-military-exercise-and-manipulate-troops-it-wasnt-very-hard-to-do/

Fleischer, D. (2016). *Wirtschaftsspionage: Phänomenologie - Erklärungsansätze - Handlungsoptionen*. Springer Vieweg.

Foozy, C. F., Ahmad, R., Yusof, R., Abdollah, F., & Masud, M. (2012). *Generic Taxonomy of Social Engineering Attack and Defence Mechanism for Handheld Computer Study*. https://www.semanticscholar.org/paper/Generic-Taxonomy-of-Social-Engineering-Attack-and-Foozy-Ahmad/cfa263c4584e3357e351a657a6472ee335d1f9d8#related-papers

Fox, D. (2014). Social Engineering im Online-Banking und E-Commerce. *Datenschutz und Datensicherheit - DuD*, *38*(5), 325–328. https://doi.org/10.1007/s11623-014-0119-4

Frankfurter Allgemeine. (2020, 11). Peinlicher Fehler: Ungebetener Gast bei Videokonferenz von EU-Verteidigungsministern. *FAZ.NET*. https://www.faz.net/1.7063693

Franz, A., & Benlian, A. (2020). Spear Phishing 2.0: Wie automatisierte Angriffe Organisationen vor neue Herausforderungen stellen. *HMD Praxis der Wirtschaftsinformatik*, *57*(3), 597–612. https://doi.org/10.1365/s40702-020-00613-y

Göhner, M., & Krell, M. (2020). Qualitative Inhaltsanalyse in naturwissenschaftsdidaktischer Forschung unter Berücksichtigung von Gütekriterien: Ein Review. *Zeitschrift für Didaktik der Naturwissenschaften*, *26*(1), 207–225. https://doi.org/10.1007/s40573-020-00111-0

Grass, K. (2015). *Kriminalität: So funktioniert der Enkeltrick*. https://www.handelsblatt.com/arts_und_style/aus-aller-welt/kriminalitaet-so-funktioniert-der-enkeltrick/11462534.html

Gray, J. (2018, April 12). *Social Engineering: A Scheme as Old as Time*. Security Intelligence. https://securityintelligence.com/social-engineering-a-trick-as-old-as-time/

Gupta, S., Singhal, A., & Kapoor, A. (2016). A literature survey on social engineering attacks: Phishing attack. *2016 International Conference on Computing, Communication and Automation (ICCCA)*, 537–540. https://doi.org/10.1109/CCAA.2016.7813778

Hadnagy, C. (2011). *Die Kunst des Human Hacking* (2011. Aufl.). mitp-Verlag.

Hatfield, J. M. (2018). Social engineering in cybersecurity: The evolution of a concept. *Computers & Security*, *73*, 102–113. https://doi.org/10.1016/j.cose.2017.10.008

Heinrich, L. J., Heinzl, A., & Riedl, R. (2011). *Wirtschaftsinformatik: Einführung und Grundlegung* (4., überarb. und erw. Aufl). Springer.

Helfferich, C. (2019). Leitfaden- und Experteninterviews. In N. Baur & J. Blasius (Hrsg.), *Handbuch Methoden der empirischen Sozialforschung* (S. 669–686). Springer Fachmedien Wiesbaden. https://doi.org/10.1007/978-3-658-21308-4_44

Internet Crime Complaint Center (IC3) | Business Email Compromise The $26 Billion Scam. (2019). https://www.ic3.gov/Media/Y2019/PSA190910#fn1

IONOS; Social Engineering: Sicherheitslücke Mensch. (2020, Mai 15). IONOS Digitalguide. https://www.ionos.at/digitalguide/server/sicherheit/social-engineering-die-sicherheitsluecke-auf-layer-8/

Irwin, L. (2020, Juli 27). *ISO 27001: The 14 Control Sets of Annex A Explained*. IT Governance UK Blog. https://www.itgovernance.co.uk/blog/iso-27001-the-14-control-sets-of-annex-a-explained

ISO 27001: Standardisierte Norm zur Informationssicherheit in Unternehmen. (2021). IONOS Digitalguide. https://www.ionos.at/digitalguide/server/sicherheit/iso-27001/

Jamil, A., Asif, K., Ghulam, Z., Nazir, M. K., Mudassar Alam, S., & Ashraf, R. (2018). MPMPA: A Mitigation and Prevention Model for Social Engineering Based Phishing attacks on Facebook. *2018 IEEE International Conference on Big Data (Big Data)*, 5040–5048. https://doi.org/10.1109/BigData.2018.8622505

Kaiser, R. (2014). *Qualitative Experteninterviews: Konzeptionelle Grundlagen und praktische Durchführung*. Springer VS.

Khin, D. (2016). *From Being Hunted By The FBI To Working Alongside Them-Kevin Mitnick*. https://www.appknox.com/blog/kevin-mitnick

Klipper, S. (2020). Weird Sociotechnical Systems. *HMD Praxis der Wirtschaftsinformatik*, *57*(3), 571–583. https://doi.org/10.1365/s40702-020-00606-x

Luber, S. (2017). *Was ist ein CISO / CSO?* https://www.security-insider.de/was-ist-ein-ciso-cso-a-672819/

Luber, S., & Schmitz, P. (2017a). *Was ist ein Penetrationstest?* https://www.security-insider.de/was-ist-ein-penetrationstest-a-667683/

Luber, S., & Schmitz, P. (2017b, April 3). *Was ist ein Hacker?* https://www.security-insider.de/was-ist-ein-hacker-a-596399/

Maan, P. S., & Sharma, M. (2012). Social Engineering: A Partial Technical Attack. *IJCSI International Journal of Computer Science Issues*, *Vol.9*.

Mayring, P. (2015). *Qualitative Inhaltsanalyse: Grundlagen und Techniken* (12., überarbeitete Auflage). Beltz Verlag.

Möhring, A. (2020). *Phishing-Mails erkennen und richtig handeln*. Tipps & Tricks. https://www.heise.de/tipps-tricks/Phishing-Mails-erkennen-und-richtig-handeln-3974927.html

Mouton, F., Leenen, L., & Venter, H. S. (2016, Dezember). Social Engineering Attack Examples, Templates and Scenarios. *Computers & Security*.

Nathaniel, S. (2018). *The History and Evolution of Social Engineering Attacks*. https://commissum.com/blog-articles/the-history-and-evolution-of-social-engineering-attacks

Nguyen, T. H., & Bhatia, S. (2020). Higher Education Social Engineering Attack Scenario, Awareness & Training Model. *Journal of The Colloquium for Information Systems Security Education*, *8*(Fall 2020).

Österreichisches Informationssicherheitshandbuch. (2020a). https://www.sicherheitshandbuch.gv.at/siha.php

Österreichisches Informationssicherheitshandbuch. (2020b). https://www.onlinesicherheit.gv.at/Themen/Experteninformation/Handbuecher/Informationssicherheitshandbuch.html

Österreichisches Informationssicherheitshandbuch. (2021). https://www.sicherheitshandbuch.gv.at/siha.php#323

Pagani, P. (2020). *The Most Common Social Engineering Attacks [Updated 2020]*. Infosec Resources. https://resources.infosecinstitute.com/topic/common-social-engineering-attacks/

Phishing Activity Trends Report (Nr. 2). (2020). APWG.

Phishing ENISA Threat Landscape. (2020). Enisa.

Pokupec, D., & Schmitz, P. (2020). *Psychisches Hacking der „Schwachstelle Mensch"*. https://www.security-insider.de/psychisches-hacking-der-schwachstelle-mensch-a-912554/

PwC. (2020). *Die neue Rolle des CISO* -. 5.

Quinlan, L. (2020). *A Solution for Human Vulnerabilities to Social Engineering Attacks: The Social Engineering Defence Model*. https://doi.org/10.13140/RG.2.2.35328.66562

Reifegradmodelle. (2021). Bundesamt für Sicherheit in der Informationstechnik. https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/IT-Grundschutz/Zertifizierte-Informationssicherheit/IT-Grundschutzschulung/Online-Kurs-IT-Grundschutz/Lektion_9_Aufrechterhaltung/9_04_Reifegradmodelle.html;jsessionid=D82EE594E677384E0E7294E185A16C36.internet081?nn=439806

Ries, U. (2013). *Black Hat: Maltego wird angriffslustig*. Security. https://www.heise.de/security/meldung/Black-Hat-Maltego-wird-angriffslustig-1928175.html

Salahdine, F., & Kaabouch, N. (2019). Social Engineering Attacks: A Survey. *Future Internet*, *11*(4), 89. https://doi.org/10.3390/fi11040089

Saurugg, H. (2007). Social Engineering & Co. - Vertrauen und Offenheit contra Geheimnisverrat. *TRUPPENDIENST*, *2/2007*. http://www.bundesheer.at/truppendienst/ausgaben/artikel.php?id=567

Schneier, B. (2019). *Attacking Soldiers on Social Media—Schneier on Security*. https://www.schneier.com/blog/archives/2019/02/attacking_soldi.html

Schumacher, M. (2013). *Hacker contest: Sicherheitsprobleme, Lösungen, Beispiele*. Springer.

Schumacher, S. (2014). Die psychologischen Grundlagen des Social-Engineerings. *Information - Wissenschaft & Praxis*, *65*(4–5). https://doi.org/10.1515/iwp-2014-0039

Schwan, B. (2008). *Kevin Mitnick sieht Social Engineering weiter als größtes Sicherheitsproblem*. Technology Review. https://www.heise.de/newsticker/meldung/Kevin-Mitnick-sieht-Social-Engineering-weiter-als-groesstes-Sicherheitsproblem-215357.html

SOCIAL ENGINEERING | Bedeutung im Cambridge Englisch Wörterbuch. (2020). https://dictionary.cambridge.org/de/worterbuch/englisch/social-engineering

Spies and Espionage. (2020). *Security Through Education*. https://www.social-engineer.org/framework/general-discussion/categories-social-engineers/spies-espionage/

State of the Phish 2020. (2020). proofpoint.

Sun Tzu. (o. J.). *Die Kunst des Krieges*.

Thai, N., & Sajal, B. (2020). Higher Education Social Engineering Attack Scenario, Awareness &Training Model. *Journal of The Colloquium for Information System s Security Education*, *8*.

Vanian, J. (2021). *Data from half a billion LinkedIn users has been scraped and put online*. Fortune. https://fortune.com/2021/04/08/linkedin-user-data-breach-leak-hackers/

VERIZON Data Breach Investigations Report 2020. (2020). VERIZON.

Was ist ein Whaling-Angriff? (2021, Januar 13). www.kaspersky.de. https://www.kaspersky.de/resource-center/definitions/what-is-a-whaling-attack

Was ist Vishing? (2021, Januar 29). www.kaspersky.de. https://www.kaspersky.de/resource-center/definitions/vishing

Was macht einen CISO aus: Erfolg und Führungsverhalten im Bereich IT-Sicherheit in Unternehmen. (2018). Kaspersky Lab.

Watering Hole—Website Attacke | Proofpoint DE. (2016, September 8). Proofpoint. https://www.proofpoint.com/de/threat-reference/watering-hole

Weber, K., Schütz, A. E., & Fertig, T. (2020). Insider Threats – Der Feind in den eigenen Reihen. *HMD Praxis der Wirtschaftsinformatik*, *57*(3), 613–627. https://doi.org/10.1365/s40702-020-00616-9

Welche Aufgaben ein CISO übernehmen muss. (2021). https://www.security-insider.de/welche-aufgaben-ein-ciso-uebernehmen-muss-a-800274/

Witt, B. (2006). Risikomanagement. In *IT-Sicherheit kompakt und verständlich* (S. 91–129). Vieweg. https://doi.org/10.1007/978-3-8348-9077-1_3

Witzel, A. (2000). *Das problemzentrierte Interview* (S. 463–475). Gabler. https://doi.org/10.1007/978-3-8349-9441-7_29

Wright, R. (2016, Juni). *Frank Abagnale: No technology can beat a social engineering attack*. SearchCloudSecurity. https://searchcloudsecurity.techtarget.com/news/450297978/Frank-Abagnale-No-technology-can-beat-a-social-engineering-attack

10 Abbildungsverzeichnis

11 Tabellenverzeichnis

Autor:

Michael SUKER, BSc MSc
michael.suker@bmlv.gv.at
Leiter Cyber Dokumentations- und Forschungszentrum
der Zentraldokumentation/ Landesverteidigungsakademie.

Die Schwerpunkte des Cyberdokumentations- und Forschungszentrums (CDFZ) liegen bei der Forschung und Entwicklung von Cyber-relevanten Themen und der Beschaffung von weltweiten Cybernachrichten auf Basis offener Quellen. Die Cybersoldaten des CDFZ verfügen über umfassende Kenntnisse in Bezug auf Informationstechnologie sowie Sprachkenntnissen, um aus dem breiten Themenfeld bei der Erstellung und Auswertung eines umfassenden Cyberlagebildes maßgeblich zu unterstützen.

Lektorat:

Mag. Rudolf BOGENSPERGER Bakk.
rudolf.bogensperger@bmlv.gv.at
Referent Allgemeine Dokumentation
der Zentraldokumentation/ Landesverteidigungsakademie

Band 9 / 2021

Der ständige Zuwachs neuer Technologien und IKT-Systeme bringt nicht nur Vorsprung und Gewinn.

Sie gefährden vor allem die Informationssicherheit. Technische Abwehrmaßnahmen werden kontinuierlich neu entwickelt, um Einfallstore für Angriffe bestmöglich zu schließen. Leider wird der Mensch als wesentlicher Faktor der Informationssicherheit wenig beachtet.

Diese Angriffsart, die durch geschickte Täuschung und Manipulation des Menschen vorhandene technische Schutzmaßnahmen umgeht, nennt sich Social Engineering.

Diese Studie beschäftigt sich mit der explorativen Fragestellung, warum Unternehmen trotz umgesetzter Schulungsmaßnahmen Opfer von Social Engineering Angriffen werden. Es werden abschließend organisatorische Handlungsempfehlungen für Unternehmen und Organisationen abgeleitet.

ISBN: 978-3-903359-33-8